

# **THEODORE ROOSEVELT AMERICAN INN OF COURT**

**May 24, 2018 @ 5:30 p.m.**

**Cybersecurity – How to Commit Malpractice and Not Even Know It**

**CLE: 1 hour of professional practice, 1 hour of ethics**

Michael Cardello III, Esq.

Juan Luis Garcia, Esq.

Danielle B. Gatto, Esq.

Steven S. Rubin, Esq.

Stephen Treglia, Esq.

Hon. Ira B. Warshawsky

Domenick Pesce

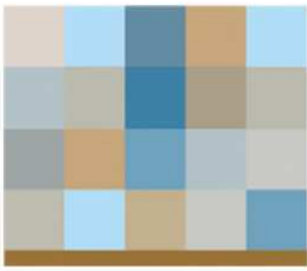
# **THEODORE ROOSEVELT AMERICAN INN OF COURT**

**May 24, 2018 @ 5:30 p.m.**

## **Cybersecurity – How to Commit Malpractice and Not Even Know It**

### **Program Agenda**

Encryption Issues	5 minutes
Ethical Considerations	20 minutes
DFS Implications	10 minutes
Ransomware and Spear Phishing	10 minutes
Privilege Issues	5 minutes
HIPAA Implications	15 minutes
SEC and FTC Implications	10 minutes
GDPR Implications	5 minutes
Cybersecurity Insurance	20 minutes



# ALERT

**April 2017**

## **Encryption: Taking A Step Towards Limiting Legal Liability For A Data Breach**

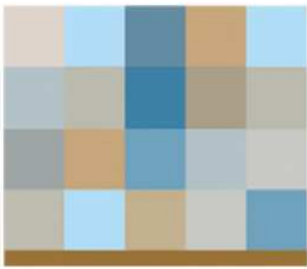
The challenges that come along with securing sensitive information are unprecedented. It has become extremely difficult to protect data which is stored electronically, and breaches have unfortunately become a frequent occurrence. It is now legally required that companies take *some* steps to protect their sensitive data. With that being said, there are many different measures available to choose from. The array of options may leave companies confused or overwhelmed not knowing where to begin. If you are unable to figure out where to begin, consider starting with encryption.

Encryption is both an easy and comprehensible starting point. Encryption, in the most basic sense, is a method used to encode your data. The process converts plain text to encrypted text with the use of an encryption key that is only given to authorized users. Authorized personnel then use the key to decipher the coded information. Without knowledge of the encryption key, one cannot comprehend the encrypted text, and instead will be left with meaningless characters that unauthorized users are unable to decode.

Encryption provides far more than a platform of frustration and failure for potential hackers. Instead, it serves a dual function. Firstly, encryption provides a layer of protection for your company's data. Secondly, encryption may be the key in avoiding liability in certain situations.

The laws which govern technology are still continuing to evolve. Technology develops at an incredible pace, leaving courts and legislatures trying to catch up. As a result, the legal standard used to hold companies liable for sensitive data being disseminated is still in a state of flux. Courts however have suggested that if a company takes steps to encrypt their data, they may be able to avoid liability if a breach should later occur.

Thus far, it seems the courts have decided the *reasonableness* standard will govern in data breach liability. Essentially, they look to see if the company took reasonable precautions under the circumstances to protect sensitive data. Courts tend to look at the level of sensitivity of the data, as well as the size of the organization that is in charge of securing the information. Victims who have had their private information stolen as a result of security breaches tend to seek remedies through negligence or breach of contract claims. Both actions implicate some sort of reasonableness standard. So it's no surprise that courts chose the same standard to govern companies' liability in breaches. While the waters of



# ALERT



**Moritt Hock & Hamroff LLP is a broad based commercial law firm with more than 60 lawyers and a staff of patent agents and paralegals. The firm's practice areas include: alternative dispute resolution; commercial foreclosure; commercial lending & finance; construction & surety; copyrights, trademarks & licensing; corporate & securities; creditors' rights & bankruptcy; cybersecurity; employment; equipment & transportation leasing and finance; healthcare; landlord & tenant; litigation; marketing, advertising & promotions; not-for-profit; patents; real estate; tax; and trusts & estates.**

**This Alert was written by Steven S. Rubin.**

**Mr. Rubin, a partner of the firm, chairs the firm's patent practice and co-chairs its cybersecurity practice. Mr. Rubin concentrates his practice on all phases of patent-related matters, both domestically and internationally.**

**Samantha Barbere, a legal intern with the firm, assisted with the research and preparation of this Alert.**

**Any matters raised in the Alert should be addressed to Mr. Rubin. He can be reached at (516) 873-2000 or by email at [srubin@moritthock.com](mailto:srubin@moritthock.com)**

defining the reasonableness standard remain murky, one thing is clear; companies, who store sensitive information, must do *something* to ensure its security in order to avoid liability.

Encryption is a good place to begin when trying to satisfy the threshold requirement of reasonableness. Encrypting data will render the stolen data inaccessible to hackers, and therefore reduce the chances of private information being accessed. As the effects of a breach are significantly less severe if the stolen data was encrypted, various agencies have limited or reduced potential liability in situations where stolen data was encrypted. For example, the Department of Health and Human Services (HHS) and Office for Civil Rights (OCR), both suggest that monetary penalties may be waived if sufficient encryption was used. Additionally, the Health Information Technology for Economic Clinical Health (HITECH) Act excludes healthcare entities from serious penalties for lost or stolen data if the data was encrypted prior to the breach.

There are also cases which evidence the courts willingness to mitigate an owner's liability if the stolen device was protected by encryption. For example, in May 2012, an employee at Beth Israel Deaconess Medical Center left an unencrypted personal laptop unattended on a desk in the hospital. That laptop was stolen and sensitive information electronically stored on the computer was accessed and subsequently released. The hospital was ordered to pay a \$100,000 as a result of the breach. The Court however, held that the Boston hospital could have mitigated their liability had the stolen laptop been protected by encryption.

Companies face an array of challenges when it comes to securing sensitive information effectively. This should not however, leave companies feeling powerless to these challenges. There are various options available which will provide for some degree of legal protection. Encryption is a great place to start. As noted, encryption will not only help lessen the chances of a security breach, but it may also help mitigate liability should a breach occur. It's important to remember, that although avoidance may no longer be available, taking steps to protect your data is still very much required.

◆ ◆ ◆ ◆ ◆

*This Alert is published solely for the interests of friends and clients of Moritt Hock & Hamroff LLP for informational purposes only and should in no way be relied upon or construed as legal advice.*



# AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

**Formal Opinion 477**

**May 11, 2017**

## **Securing Communication of Protected Client Information**

*A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.*

### **I. Introduction**

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for e-mail communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."<sup>1</sup>

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.<sup>2</sup>

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.<sup>3</sup>

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c)

---

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), [http://www.americanbar.org/content/dam/aba/administrative/ethics\\_2020/20120508\\_ethics\\_20\\_20\\_final\\_resolution\\_and\\_report\\_outsourcing\\_posting.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf).

3. See JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."<sup>4</sup> Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.<sup>5</sup>

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers' face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

## II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."<sup>6</sup> The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)<sup>7</sup>

---

4. "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/cybersecurity> (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

7. *Id.* at 43.

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to “keep abreast of changes in the law and its practice.” The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. <sup>8</sup>

### III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that “A lawyer shall not reveal information relating to the representation of a client” unless certain circumstances arise.<sup>9</sup> The 2012 modification added a new duty in paragraph (c) that: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”<sup>10</sup>

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

---

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), [http://www.americanbar.org/content/dam/aba/administrative/ethics\\_2020/20120808\\_revised\\_resolution\\_105a\\_as\\_amended.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf). The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.”

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.<sup>11</sup>

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

. . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.<sup>12</sup>

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).<sup>13</sup>

---

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2013). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.<sup>14</sup> Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.<sup>15</sup> "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

---

14. See item 3 below.

15. See, e.g., Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), <http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/>.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, "delete" usually does not mean information is permanently deleted, and "deleted" data may be subject to recovery. Therefore, a lawyer should consider

whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,<sup>16</sup> and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.<sup>17</sup> If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived, and the lawyer must determine whether it is prudent to warn a client of the dangers associated with such a method of communication.<sup>18</sup>

---

16. See Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

17. See, e.g., ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect the confidentiality of e-mail communications with one's client); *Scott v. Beth Israel Med. Center, Inc.*, Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); *Mason v. ILS Tech., LLC*, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); *Holmes v. Petrovich Dev Co., LLC*, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); *Bingham v. BayCare Health Sys.*, 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).

18. some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, See, e.g., Tex. Prof'l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer...;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;



5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.<sup>19</sup>

Model Rule 4.4(b) obligates a lawyer who “knows or reasonably should know” that he has received an inadvertently sent “document or electronically stored information relating to the representation of the lawyer’s client” to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer’s duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being

- 
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
  - sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

19. See *Veteran Med. Prods. v. Bionix Dev. Corp.*, Case No. 1:05-cv-655, 2008 WL 696546 at \*8, 2008 BL 51876 at \*8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read “this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed” with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.<sup>20</sup>

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including “using an Internet-based service to store client information.” Comment [3] provides that the “reasonable efforts” required by Model Rule 5.3 to ensure that the nonlawyer’s services are provided in a manner that is compatible with the lawyer’s professional obligations “will depend upon the circumstances.” Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

---

20. MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate “directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.”<sup>21</sup> If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.<sup>22</sup>

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer’s actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

#### IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.<sup>23</sup> The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, “A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.”

---

21. The ABA’s catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at:

[http://www.americanbar.org/groups/departments\\_offices/legal\\_technology\\_resources/resources/charts\\_fyis/cloud-ethics-chart.html](http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html).

22. By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, “the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer.” MODEL RULES OF PROF’L CONDUCT R. 5.3 cmt. [4] (2017). The concept of monitoring recognizes that although it may not be possible to “directly supervise” a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), [http://www.americanbar.org/content/dam/aba/administrative/ethics\\_2020/2012\\_hod\\_annual\\_meeting\\_105c\\_filed\\_may\\_2012.auth\\_checkdam.pdf](http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.auth_checkdam.pdf).

23. MODEL RULES OF PROF’L CONDUCT R. 1.4(a)(1) & (4) (2016).

## V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make “reasonable efforts” to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

---

**AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY**

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Myles V. Lynk, Tempe, AZ . John M. Barkett, Miami, FL . Arthur D. Burger, Washington, DC . Wendy Wen Yun Chang, Los Angeles, CA . Robert A. Creamer, Cambridge, MA . Hon. Daniel J. Crothers, Bismarck, ND . Keith R. Fisher, Arlington, VA . Douglas R. Richmond, Chicago, IL . Hope Cahill Todd, Washington, DC . Allison Wood, Chicago, IL

**CENTER FOR PROFESSIONAL RESPONSIBILITY:** Dennis A. Rendleman, Ethics Counsel;  
Mary McDermott, Associate Ethics Counsel

©2017 by the American Bar Association. All rights reserved.



# ETHICS OPINION 1020

---

**New York State Bar Association  
Committee on Professional Ethics**

Opinion 1020 (9/12/2014)

**Topic:** Confidentiality; use of cloud storage for purposes of a transaction

**Digest:** Whether a lawyer to a party in a transaction may post and share documents using a “cloud” data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

**Rules:** 1.1, 1.6

## FACTS

1. The inquirer is engaged in a real estate practice and is looking into the viability of using an electronic project management tool to help with closings. The technology would allow sellers’ attorneys, buyers’ attorneys, real estate brokers and mortgage brokers to post and view documents, such as drafts, signed contracts and building financials, all in one central place.

## QUESTION

2. May a lawyer representing a party to a transaction use a cloud-based technology so as to post documents and share them with others involved in the transaction?

## OPINION

3. The materials that the inquirer seeks to post, such as drafts, contracts and building financials, may well include confidential information of the inquirer’s clients, and for purposes of this opinion we assume that they do.<sup>1</sup> Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer’s ethical duty to preserve a client’s confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client’s informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer “exercise reasonable care to prevent ... [persons] whose services are utilized by the lawyer from disclosing or using confidential information of a client.”

5. Comment [17] to Rule 1.6 addresses issues raised by a lawyer’s use of technology:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

6. In the recent past, our Committee has repeatedly been asked to provide guidance on the interplay of technology and confidentiality. N.Y. State 1019 (2014) catalogues the Committee's opinions on technology. In that opinion, we considered whether a law firm could provide its lawyers with remote access to its electronic files. We concluded that a law firm could use remote access "as long as it takes reasonable steps to ensure that confidential information is maintained." *Id.* ¶12
7. Similarly, in N.Y. State 842 (2010), which considered the use of cloud data storage, we concluded that a lawyer could use this technology to store client records provided that the lawyer takes reasonable care to protect the client's confidential information. We also reached a similar conclusion in N.Y. State 939 (2012) as to the issue of lawyers from different firms sharing a computer system.
8. The concerns presented by the current inquiry were also present in N.Y. State 1019, N.Y. State 939 and N.Y. State 842, and those opinions govern the outcome here. That is, the inquirer may use the proposed technology provided that the lawyer takes reasonable steps to ensure that confidential information is not breached.<sup>2</sup> The inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared. Because of the fact-specific and evolving nature of technology, we do not purport to specify in detail the steps that will constitute reasonable care in any given set of circumstances. See N.Y. State 1019. ¶10. We note, however, that use of electronically stored information may not only require reasonable care to protect that information under Rule 1.6, but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.<sup>3</sup>
9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

## CONCLUSION

10. Whether a lawyer for a party in a transaction may post and share documents using a “cloud” data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

(17-14)

<sup>1</sup>Rule 1.6(a) defines “confidential information” generally to include “information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential.”

<sup>2</sup>This result is consistent with results in other jurisdictions that have considered lawyers’ use of off-site, third-party cloud services for storing and sharing documents. *See, e.g.*, ABA 95-398; Arizona Opinion 05-04; California Opinion 2010-179; Connecticut Inf. Opinion 2013-07; Florida Opinion 12-3 (2013); Illinois Opinion 10-01 (2009); Iowa Opinion 11-01; Maine Opinion 207 (2013); Massachusetts Opinion 12-03; Massachusetts Opinion 05-04; Missouri Inf. Opinion 2006-0092; Nebraska Opinion 06-05; New Hampshire Opinion 2012-13/4 (2013); New Jersey Opinion 701 (2006); North Carolina Opinion 2011-6 (2012); North Dakota Opinion 99-03 (1999); Ohio Opinion 2013-03; Oregon Opinion 2011-188; Pennsylvania Opinion 2011-200; Pennsylvania Opinion 2010-060; Vermont Opinion 2010-6 (2012); Washington Inf. Opinion 2215 (2012).

<sup>3</sup>It has been said for example that the duty of competence may require litigators, depending on circumstances, to possess a basic or even a more refined understanding of electronically stored information. *See, e.g.*, Zachary Wang, “Ethics and Electronic Discovery: New Medium, Same Problems,” 75 Defense Counsel Journal 328, at 7 (October 2008) (“disclosure of privileged information as a result of a lack of knowledge of a client’s IT system would subject an attorney to discipline under Rules 1.1 and 1.6”). The California State Bar Standing Committee on Professional Responsibility and Conduct has tentatively approved an interim opinion interpreting California ethical rules as follows:

Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information (“ESI”). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. ... An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.



One Elk Street, Albany , NY 12207

**Phone:** 518-463-3200 **Secure Fax:** 518.463.5993

© 2015 New York State Bar  
Association

**New York County Lawyers Association Professional Ethics Committee**

**Formal Opinion 749**

**February 21, 2017**

**TOPIC:** A lawyer's ethical duty of technological competence with respect to the duty to protect a client's confidential information from cybersecurity risk and handling e-discovery when representing clients in a litigation or government investigation.

**DIGEST:** A lawyer's ethical duty of competence extends to the manner in which he provides legal services to the client as well as the lawyer's substantive knowledge of the pertinent areas of law. The duty of competence expands as technological developments become integrated into the practice of law. Lawyers should be aware of the disclosure risks associated with the transmission of client confidential information by electronic means, and should possess the technological knowledge necessary to exercise reasonable care with respect to maintaining client confidentiality and fulfilling e-discovery demands. Further, a lawyer's duty of competence in a litigation or investigation requires that the lawyer have a sufficient understanding of issues relating to securing, transmitting, and producing electronically stored information ("ESI"). The duty of technological competence required in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of technological competence if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge before performance is required, or associates with one or more persons who possess the requisite technological knowledge.

**RULES OF PROFESSIONAL CONDUCT:** 1.1, 1.6, 5.1, 5.3

**OPINION**

A lawyer has a duty to "provide competent representation to a client," which requires that the lawyer demonstrate "the legal knowledge, skill, thoroughness and preparation necessary for the representation." New York Rules of Professional Conduct ("RPCs"), RPC 1.1. A comment to the rule notes that "[t]o maintain the requisite knowledge and skill, a lawyer should . . . (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." RPC 1.1, Cmt. [8]. RPC 1.6 provides that a lawyer "shall not knowingly reveal confidential information, as defined in this RPC, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person." RPC 1.6(c) further requires a lawyer to "exercise reasonable care to prevent disclosure of information related to the representation by employees, associates and others whose services are utilized in connection with the representation."

**Duty of Competence and Protection of Electronically Transmitted Client**

## Information

Compliance with RPC 1.6 requires that lawyers who use technology to store or transmit a client's confidential information, or to communicate with clients, use reasonable care with respect to those uses. The lawyer must assess the risks associated with the use of that technology to determine if the use is appropriate under the circumstances. *See, e.g.*, N.Y. State 709 (1998) ("an attorney must use reasonable care to protect confidences and secrets"); N.Y. City 94-11 (lawyer must take reasonable steps to secure client confidences and secrets). Lawyers should be aware that the storage and transmission of a client's confidential information electronically carries a risk of disclosure if the stored or transmitted data is hacked, or if human, software or hardware error results in an inadvertent disclosure.

Attacks on computer systems by those trying to gain confidential, proprietary, or other sensitive information for personal or political gain (including so-called "hacktivists") are reported with alarming frequency. Corporate clients have become proactive in attempting to ensure that its outside vendors—including lawyers—who have access to sensitive corporate information sufficiently protect that information from disclosure through inadvertence or cyber-attack. Individual clients are increasingly sensitive to the potential harm from widely reported data breaches, and similarly expect their lawyers to use appropriate measures to avoid unauthorized disclosure of personal data. In response to these concerns, at least 25 states have adopted rules regarding maintaining technological competence, including most recently Florida's rule, which mandates continuing legal education on the subject. *See, e.g.*, Florida Rules of Professional Conduct, Rule 6-10.3(b) (effective January 1, 2017, a Florida lawyer's CLE requirements will include 3 credit hours in approved technology programs); California Standing Committee on Professional Responsibility and Conduct Formal Op. 2015-193 (concluding that an attorney lacking the required e-discovery competence must either acquire the requisite skill before performance is required, associate with technical consultants or competent counsel, or decline the representation). An overwhelming majority of lawyers recently surveyed who work in firms ranging from solo practitioners to over 500 attorneys believed training in the firm's technology is important.<sup>1</sup>

Additionally, lawyers who represent clients who are located outside of New York may, in certain instances, be subject to laws in those other states that require a heightened level of protection of electronic communications. *See, e.g.*, Mass. Gen. L. Ch. 93H, 201 C.M.R. 17 (requiring, where technically feasible, the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly); Nevada Senate Bill 227 (amending Nev. Rev. Stat. § 597.970 and requiring that data collectors who conduct business in the state encrypt data storage devices – including computers, cell phones and thumb drives – that contain personal information that are moved outside the secured physical and logical boundaries of the data collecting

---

<sup>1</sup> "2016 Legal Technology Survey Report," American Bar Association (2016).

entity).

Lawyers must have a sufficient understanding of the technology – either directly or through associating with persons possessing such knowledge – to determine how to satisfy the lawyer’s duty of reasonable care. Reasonable care will vary depending on the circumstances, including the subject matter, the sensitivity of the information, the likelihood that the information is sought by others, and the potential harm from disclosure. *See* NYCLA Op. 738 (2008) (lawyer may not ethically search metadata made available through an adversary’s inadvertent disclosure of client confidential information through metadata); N.Y. State 782 (2004) (addressing the exercise of reasonable care to prevent the disclosure of client confidential information through metadata).

### **Duty of Competence and Electronically Stored Information**

Lawyers who represent client in litigations, or in government or regulatory investigations, are well aware that often a significant aspect of the representation of the client is the collection, preservation and production of ESI. The ethical duty of competence requires an attorney to assess at the outset of e-discovery issues that may arise in the course of the representation, including the likelihood that e-discovery will or should be sought by either side, identification of likely electronic document custodians, and preservation and collection of potentially relevant ESI in an appropriate database that will permit the lawyer to search for responsive ESI during e-discovery.

A lawyer’s obligations with respect to ESI will be governed by applicable state or federal law. *See, e.g.,* Fed. R. Civ. P. Rules 16, 26 and 37 (outlining a federal court litigant’s obligations with respect to the presentation and production of ESI); Rules 202.12(b) and 202.70(g) of New York’s Uniform Trial Court Rules (requiring all attorneys be sufficiently versed in matters relating to their client’s technological systems to be competent to discuss all issues relating to electronic discovery at preliminary conferences). In addition, a lawyer’s ethical duty of competence requires the lawyer to assess his or her own e-discovery skills and resources in order to meet these ESI demands. E-discovery needs in a particular matter may include (i) assessing e-discovery needs and ESI preservation procedures; (ii) identifying custodians of potentially relevant ESI; (iii) understanding the client’s ESI system and storage; (iii) determining and advising the client on alternatives for the collection and preservation of ESI and associated costs; and (v) ensuring that the collection procedures, software and/or databases created will permit the lawyer to provide responsive ESI in an appropriate manner. If a lawyer lacks the requisite skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate with another attorney or expert who possess these skills. RPC 1.1 (b) & Cmt., 1,Cmt. 8.

Where a lawyer satisfies his or her duty of technological competence by associating with another lawyer or expert, the lawyer remains responsible for fulfilling the duty of

competence, and must satisfy himself or herself that the work of the associated lawyer or expert is being done properly. The lawyer must understand the pertinent legal issues and the e-discovery obligations imposed by law or court order and the relevant risks associated with the e-discovery tasks at hand, and satisfy himself or herself that everyone involved in the e-discovery process on behalf of the client is conducting themselves accordingly. *See* RPCs 5.1, 5.3.

## CONCLUSION

A lawyer's ethical duty of competence extends to the manner in which he or she provides legal services to the client as well as the lawyer's substantive knowledge of the relevant areas of law. Lawyers must be responsive to technological developments as they become integrated into the practice of law. A lawyer cannot knowingly reveal client confidential information, and must exercise reasonable care to ensure that the lawyer's employees, associates and others whose services are utilized by the lawyer not disclose or use client confidential information. The risks associated with transmission of client confidential information electronically include disclosure through hacking or technological inadvertence. A lawyer's duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology where the practice requires the use of technology to competently represent the client.

A lawyer's competence with respect to litigation requires that the lawyer possesses a sufficient understanding of issues relating to securing, transmitting, and producing ESI. The duty of competence in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of competence with respect to technology if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge in a timely manner and before performance is required, or associates with one or more persons who possess the requisite technological knowledge. If a lawyer is unable to satisfy the duty of technological competence associated with a matter, the lawyer should decline the representation.

**NEW YORK STATE  
DEPARTMENT OF FINANCIAL SERVICES  
23 NYCRR 500**

**CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES**

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

**(ALL MATTER IS NEW)**

**Section 500.00 Introduction.**

The New York State Department of Financial Services (“DFS”) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

**Section 500.01 Definitions.**

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

- (1) Knowledge factors, such as a password; or
- (2) Possession factors, such as a token or text message on a mobile phone; or
- (3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.



(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

## **Section 500.02 Cybersecurity Program.**

(a) *Cybersecurity Program*. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

### **Section 500.03 Cybersecurity Policy.**

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

- (j) physical security and environmental controls;
- (k) customer data privacy;
- (l) vendor and Third Party Service Provider management;
- (m) risk assessment; and
- (n) incident response.

#### **Section 500.04 Chief Information Security Officer.**

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

- (1) retain responsibility for compliance with this Part;
- (2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
- (3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

- (1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
- (2) the Covered Entity's cybersecurity policies and procedures;
- (3) material cybersecurity risks to the Covered Entity;
- (4) overall effectiveness of the Covered Entity's cybersecurity program; and
- (5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

#### **Section 500.05 Penetration Testing and Vulnerability Assessments.**

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

#### **Section 500.06 Audit Trail.**

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

#### **Section 500.07 Access Privileges.**

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

#### **Section 500.08 Application Security.**

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

#### **Section 500.09 Risk Assessment.**

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

#### **Section 500.10 Cybersecurity Personnel and Intelligence.**

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

#### **Section 500.11 Third Party Service Provider Security Policy.**

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible

to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

## **Section 500.12 Multi-Factor Authentication.**

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

### **Section 500.13 Limitations on Data Retention.**

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

### **Section 500.14 Training and Monitoring.**

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

### **Section 500.15 Encryption of Nonpublic Information.**

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

### **Section 500.16 Incident Response Plan.**

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;



- (2) the goals of the incident response plan;
- (3) the definition of clear roles, responsibilities and levels of decision-making authority;
- (4) external and internal communications and information sharing;
- (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
- (7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

#### **Section 500.17 Notices to Superintendent.**

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- (1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

#### **Section 500.18 Confidentiality.**

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

#### **Section 500.19 Exemptions.**

- (a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than \$5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than \$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

#### **Section 500.20 Enforcement.**

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

#### **Section 500.21 Effective Date.**

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

#### **Section 500.22 Transitional Periods.**

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

#### **Section 500.23 Severability.**

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

APPENDIX A (Part 500)

---

(Covered Entity Name)

February 15, 20\_\_\_\_

**Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations**

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of\_\_\_\_\_(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended\_\_(year for which Board Resolution or Compliance Finding is provided) complies with Part \_\_\_\_.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)\_\_\_\_\_

Date: \_\_\_\_\_

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

\_\_\_\_\_  
(Covered Entity Name)

(Date)\_\_\_\_\_

**Notice of Exemption**

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)\_\_\_\_\_

Date: \_\_\_\_\_

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]

# CYBERSECURITY & DATA PROTECTION SERVICES

**Cyber-attacks continue to grow in size and creativity, and they are disrupting businesses of all types and sizes. More data was lost or stolen in the first half of 2017 (1.9 billion records) than in the entire year of 2016 (1.37 billion)<sup>1</sup>.**

## MARKET VIEW

Financial service firms must be proactive and continually improve their attack readiness to reduce cyber risk and minimize potential impacts.

## SOLUTION

Cordium's Cybersecurity & Data Protection Consulting Services are designed to assist financial firms in assessing their cybersecurity risks, threats, and preparedness against a cyber incident, and potential consequences should an incident occur.

### CYBERSECURITY ASSESSMENT

Our team of experts will identify your firms' priorities and establish an appropriate governance framework, and supporting policies and procedures by conducting cybersecurity risk assessments, penetration testing, and vulnerability scans. We can also conduct a gap analysis and maturity assessment to identify control weaknesses and areas for improvement.

### POLICY REVIEW AND DEVELOPMENT

Once an evaluation of your cybersecurity readiness is determined we can help you develop a strategic plan appropriate for your firm's risk tolerance and resources. We will review your firm's information security policies and procedures and compare them against your regulatory requirements and the National Institute of Standards and Technology (NIST) framework to ensure optimal preparedness.

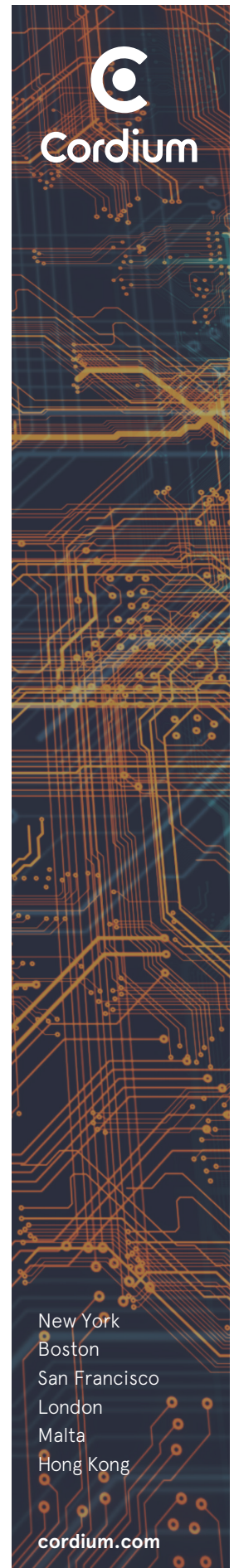
### VENDOR RISK MANAGEMENT

Our team can help you to establish an effective Vendor and Third Party Risk Management Program as well as conduct due diligence on vendors and third parties to ensure their cybersecurity controls meet your organization's requirements.

### VIRTUAL CISO

Cordium can act as a virtual CISO to free up your employees to focus on your business instead of cyber concerns. Our team can facilitate cyber-attack incident response simulation exercises to help improve response capabilities and minimize impact and reputational damage. We can provide employee training to increase cyber-attack awareness and minimize the risk of a cyber-attack through human error. We can also develop policy and procedure control testing plans. E.g. patching, access controls, data loss prevention, etc.

<sup>1</sup><https://blog.gemalto.com/security/2018/01/18/2017-year-ransomware/>



# NYDFS CONSULTING SERVICES

**Cybersecurity is one of the fastest growing challenges for financial services firms. The cyber threat landscape continues to expand, and regulatory requirements and scrutiny are increasing.**

## MARKET VIEW

In September of 2016, New York was the first state to rollout mandated regulation in relation to cybersecurity. This regulation requires banks, insurance companies, and other financial firms regulated by the New York State Department of Financial Services (NYDFS) to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness financial industry in New York.

## SOLUTION

Cordium's Cybersecurity and Data Protection Consulting Services are designed to identify and manage potential cyber risks and threats as well as provide clients with regulatory and compliance support. We have developed a practical and cost-effective approach in-line with NYDFS regulatory requirements.

### CYBERSECURITY CONTROLS IMPLEMENTATION- INHERENT RISK PROFILE AND CYBERSECURITY MATURITY LEVEL ASSESSMENT

Our assessment provides practical recommendations to close control gaps, improve control maturity, and mitigate risks. We review the firm's information security policies, standards, and procedures against the NIST Cybersecurity Framework, and regulatory requirements using the FFIEC Cybersecurity Assessment Tool (CAT). We also administer IT staff interviews and workshops to gain an understanding of the firm's cybersecurity governance.

### CYBERSECURITY RISK, THREAT, IMPACT, AND PROGRAM DESIGN ASSESSMENT

Individual or workshop-based interviews with senior leadership and department heads to identify and create leadership awareness of the firm's cyber risks, threats, and potential impact if they are compromised.

### CYBERSECURITY STRATEGIC PLAN ASSESSMENT

Provide a "risk-based" approach to mitigation and acceptance, Cordium will identify and align cybersecurity projects and initiatives with the firm's identified cyber threats and vulnerabilities. We assess, revise, or create the firm's current cybersecurity strategic plan, and evaluate alignment of information technology security projects. This ensures initiatives are properly aligned with the firm's identified cyber risks, threats, vulnerabilities, and potential impact.

New York  
Boston  
San Francisco  
London  
Malta  
Hong Kong

[cordium.com](http://cordium.com)

## NYDFS CONSULTING SERVICES

### TIMELINE

#### \*ANNUAL REQUIREMENTS

**OCTOBER 31 – NOVEMBER 1**

FS-ISAC Cyber Exercise

**FEBRUARY 15**

Sign & submit Certification of Compliance to NYDFS

2017

AUGUST 28

- ☒ Cybersecurity program aligned to NIST Cybersecurity Framework
- ☒ Cybersecurity policy
- ☒ Review / Assign access privileges
- ☒ CISO / 3rd party designation
- ☒ Sufficient staffing / training
- ☒ Written Incident Response Plan
- ☒ Reporting incidents to NYDFS in 72 hrs

2018

MARCH 1

- ☒ Written report to Board by CISO
- ☒ Perform annual pen test, biannual vulnerability scans
- ☒ Perform annual cyber risk assessment
- ☒ Enact multi-factor authentication for external access to internal systems

SEPTEMBER 1

- ☐ Audit trail for tracking/maintaining data for at least 6 yrs
- ☐ Implement Application Security Policies & Procedures for secure development practices
- ☐ Documentation for timely destruction of non-public information
- ☐ Implement policies & procedures for monitoring authorized users and unauthorized activity
- ☐ Encrypt all non-public information in transit and at rest

2019

MARCH 1

- ☐ Establish 3rd party Information Security Policy which includes annual review of 3rd parties

### ABOUT CORDIUM

Cordium is a market-leading provider of governance, risk and compliance services to the asset management and securities industry. Cordium has offices in London, New York, Boston, San Francisco, Malta and Hong Kong. The firm employs more than 200 experienced professionals who support over 1,500 clients in the financial services industry.

New York  
Boston  
San Francisco  
London  
Malta  
Hong Kong

[cordium.com](http://cordium.com)



**PRECEDENTIAL**

UNITED STATES COURT OF APPEALS  
FOR THE THIRD CIRCUIT

---

No. 14-3514

---

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORPORATION,  
a Delaware Corporation  
WYNDHAM HOTEL GROUP, LLC,  
a Delaware limited liability company;  
WYNDHAM HOTELS AND RESORTS, LLC,  
a Delaware limited liability company;  
WYNDHAM HOTEL MANAGEMENT INCORPORATED,  
a Delaware Corporation

Wyndham Hotels and Resorts, LLC,  
Appellant

---

On Appeal from the United States District Court  
for the District of New Jersey  
(D.C. Civil Action No. 2-13-cv-01887)  
District Judge: Honorable Esther Salas

---

Argued March 3, 2015

Before: AMBRO, SCIRICA, and ROTH, Circuit Judges

(Opinion filed: August 24, 2015)

Kenneth W. Allen, Esquire  
Eugene F. Assaf, Esquire (Argued)  
Christopher Landau, Esquire  
Susan M. Davies, Esquire  
Michael W. McConnell, Esquire  
Kirkland & Ellis  
655 15th Street, N.W., Suite 1200  
Washington, DC 20005

David T. Cohen, Esquire  
Ropes & Gray  
1211 Avenue of the Americas  
New York, NY 10036

Douglas H. Meal, Esquire  
Ropes & Gray  
800 Boylston Street, Prudential Tower  
Boston, MA 02199

Jennifer A. Hradil, Esquire  
Justin T. Quinn, Esquire  
Gibbons  
One Gateway Center  
Newark, NJ 07102

Counsel for Appellants

Jonathan E. Nuechterlein  
General Counsel  
David C. Shonka, Sr.  
Principal Deputy General Counsel  
Joel R. Marcus, Esquire (Argued)  
David L. Sieradzki, Esquire  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Washington, DC 20580

Counsel for Appellee

Sean M. Marotta, Esquire  
Catherine E. Stetson, Esquire  
Harriet P. Pearson, Esquire  
Bret S. Cohen, Esquire  
Adam A. Cooke, Esquire  
Hogan Lovells US LLP  
555 Thirteenth Street, N.W.  
Columbia Square  
Washington, DC 20004

Kate Comerford Todd, Esquire  
Steven P. Lehotsky, Esquire  
Sheldon Gilbert, Esquire  
U.S. Chamber Litigation Center, Inc.  
1615 H Street, N.W.  
Washington, DC 20062

Banks Brown, Esquire  
McDermott Will & Emery LLP  
340 Madison Ave.  
New York, NY 10713

Karen R. Harned, Esquire  
National Federation of Independent Business  
Small Business Legal Center  
1201 F Street, N.W., Suite 200  
Washington, DC 20004

Counsel for Amicus Appellants  
Chamber of Commerce of the USA;  
American Hotel & Lodging Association;  
National Federation of Independent Business.

Cory L. Andrews, Esquire  
Richard A. Samp, Esquire  
Washington Legal Foundation  
2009 Massachusetts Avenue, N.W.  
Washington, DC 20036

John F. Cooney, Esquire  
Jeffrey D. Knowles, Esquire  
Mitchell Y. Mirviss, Esquire  
Leonard L. Gordon, Esquire  
Randall K. Miller, Esquire  
Venable LLC  
575 7th Street, N.W.  
Washington, DC 20004

Counsel for Amicus Appellants  
Electronic Transactions Association,  
Washington Legal Foundation

Scott M. Michelman, Esquire  
Jehan A. Patterson, Esquire  
Public Citizen Litigation Group

1600 20th Street, N.W.  
Washington, DC 20009

Counsel for Amicus Appellees  
Public Citizen Inc.; Consumer Action;  
Center for Digital Democracy.

Marc Rotenberg, Esquire  
Alan Butler, Esquire  
Julia Horwitz, Esquire  
John Tran, Esquire  
Electronic Privacy Information Center  
1718 Connecticut Avenue, N.W., Suite 200  
Washington, DC 20009

Catherine N. Crump, Esquire  
American Civil Liberties Union  
125 Broad Street, 18th Floor  
New York, NY 10004

Chris Jay Hoofnagle, Esquire  
Samuelson Law, Technology & Public Policy Clinic  
U.C. Berkeley School of Law  
Berkeley, CA 94720

Justin Brookman, Esquire  
G.S. Hans, Esquire  
Center for Democracy & Technology  
1634 I Street N.W. Suite 1100  
Washington, DC 20006

Lee Tien, Esquire  
Electronic Frontier Foundation

815 Eddy Street  
San Francisco, CA 94109

Counsel for Amicus Appellees  
Electronic Privacy Information Center,  
American Civil Liberties Union,  
Samuelson Law, Technology & Public Policy Clinic,  
Center for Democracy & Technology,  
Electronic Frontier Foundation

---

OPINION OF THE COURT

---

AMBRO, Circuit Judge

The Federal Trade Commission Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation’s computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over \$10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham’s conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham’s motion to dismiss, and we granted interlocutory appeal on two issues:

whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision.<sup>1</sup> We affirm the District Court.

## **I. Background**

### *A. Wyndham's Cybersecurity*

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries.<sup>2</sup> Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham “manage[s]” these systems and requires the hotels to “purchase and configure” them to its own specifications. Compl. at ¶ 15, 17. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

---

<sup>1</sup> On appeal, Wyndham also argues that the FTC fails the pleading requirements of an unfairness claim. As Wyndham did not request and we did not grant interlocutory appeal on this issue, we decline to address it.

<sup>2</sup> In addition to Wyndham Worldwide, the defendant entities are Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LCC, and Wyndham Hotel Management, Inc. For convenience, we refer to all defendants jointly as Wyndham.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, “taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.” *Id.* at ¶ 24. This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain “remote access to at least one hotel’s system,” which was developed by Micros Systems, Inc., the user ID and password were both “micros.” *Id.* at ¶ 24(f).

3. Wyndham failed to use “readily available security measures”—such as firewalls—to “limit access between [the] hotels’ property management systems, . . . corporate network, and the Internet.” *Id.* at ¶ 24(a).

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented “adequate information security policies and procedures.” *Id.* at ¶ 24(c). Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham’s network even though “default user IDs and passwords were enabled . . . , which were easily available to hackers through simple Internet searches.” *Id.* And, because it failed to maintain an “adequate[] inventory [of] computers connected to [Wyndham’s] network [to] manage the devices,” it was unable to identify the source of at least one of the cybersecurity attacks. *Id.* at ¶ 24(g).



5. Wyndham failed to “adequately restrict” the access of third-party vendors to its network and the servers of Wyndham-branded hotels. *Id.* at ¶ 24(j). For example, it did not “restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary.” *Id.*

6. It failed to employ “reasonable measures to detect and prevent unauthorized access” to its computer network or to “conduct security investigations.” *Id.* at ¶ 24(h).

7. It did not follow “proper incident response procedures.” *Id.* at ¶ 24(i). The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company’s cybersecurity.

We safeguard our Customers’ personally identifiable information by using industry standard practices. Although “guaranteed security” does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for

encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain “fire walls” and other appropriate safeguards . . . .

*Id.* at ¶ 21. The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

#### *B. The Three Cybersecurity Attacks*

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham’s network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham’s network and the Internet. They then used the brute-force method—repeatedly guessing users’ login IDs and passwords—to access an administrator account on Wyndham’s network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham’s network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered “memory-scraping malware” used in the previous attack on more than thirty hotels’ computer systems. *Id.* at ¶ 34. The FTC asserts that, due to Wyndham’s “failure to monitor [the network] for

the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months.” *Id.* In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham’s cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham “had still not adequately limited access between . . . the Wyndham-branded hotels’ property management systems, [Wyndham’s network], and the Internet,” the hackers had access to the property management servers of multiple hotels. *Id.* at ¶ 37. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least \$10.6 million in fraud loss. It further states that consumers suffered financial injury through “unreimbursed fraudulent charges, increased costs, and lost access to funds or credit,” *Id.* at ¶ 40, and that they “expended time and money resolving fraudulent charges and mitigating subsequent harm.” *Id.*

### *C. Procedural History*

The FTC filed suit in the U.S. District Court for the District of Arizona in June 2012 claiming that Wyndham engaged in “unfair” and “deceptive” practices in violation of § 45(a). At Wyndham’s request, the Court transferred the case to the U.S. District Court for the District of New Jersey.

Wyndham then filed a Rule 12(b)(6) motion to dismiss both the unfair practice and deceptive practice claims. The District Court denied the motion but certified its decision on the unfairness claim for interlocutory appeal. We granted Wyndham’s application for appeal.

## **II. Jurisdiction and Standards of Review**

The District Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331, 1337(a), and 1345. We have jurisdiction under 28 U.S.C. § 1292(b).

We have plenary review of a district court’s ruling on a motion to dismiss for failure to state a claim under Rule 12(b)(6). *Farber v. City of Paterson*, 440 F.3d 131, 134 (3d Cir. 2006). In this review, “we accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.” *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002).

## **III. FTC’s Regulatory Authority Under § 45(a)**

### *A. Legal Background*

The Federal Trade Commission Act of 1914 prohibited “unfair methods of competition in commerce.” Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)). Congress “explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase ‘unfair methods of competition’ . . . by enumerating the particular practices to which it was intended to apply.” *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239–40 (1972) (citing S. Rep. No. 63-597, at 13 (1914)); *see also* S. Rep. No. 63-597, at 13 (“The committee gave *careful consideration* to

the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce . . . . It concluded that . . . there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others.” (emphasis added)). The takeaway is that Congress designed the term as a “flexible concept with evolving content,” *FTC v. Bunte Bros.*, 312 U.S. 349, 353 (1941), and “intentionally left [its] development . . . to the Commission,” *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 367 (1965).

After several early cases limited “unfair methods of competition” to practices harming competitors and not consumers, *see, e.g., FTC v. Raladam Co.*, 283 U.S. 643 (1931), Congress inserted an additional prohibition in § 45(a) against “unfair or deceptive acts or practices in or affecting commerce,” Wheeler-Lea Act, Pub. L. No. 75-447, § 5, 52 Stat. 111, 111 (1938).

For the next few decades, the FTC interpreted the unfair-practices prong primarily through agency adjudication. But in 1964 it issued a “Statement of Basis and Purpose” for unfair or deceptive advertising and labeling of cigarettes, 29 Fed. Reg. 8324, 8355 (July 2, 1964), which explained that the following three factors governed unfairness determinations:

(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes

substantial injury to consumers (or competitors or other businessmen).

*Id.* Almost a decade later, the Supreme Court implicitly approved these factors, apparently acknowledging their applicability to contexts other than cigarette advertising and labeling. *Sperry*, 405 U.S. at 244 n.5. The Court also held that, under the policy statement, the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied. *Id.*

During the 1970s, the FTC embarked on a controversial campaign to regulate children's advertising through the unfair-practices prong of § 45(a). At the request of Congress, the FTC issued a second policy statement in 1980 that clarified the three factors. FTC Unfairness Policy Statement, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Senate Comm. on Commerce, Sci., and Transp. (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) [hereinafter 1980 Policy Statement]. It explained that public policy considerations are relevant in determining whether a particular practice causes substantial consumer injury. *Id.* at 1074–76. Next, it “abandoned” the “theory of immoral or unscrupulous conduct . . . altogether” as an “independent” basis for an unfairness claim. *Int'l Harvester Co.*, 104 F.T.C. at 1061 n.43; 1980 Policy Statement, *supra* at 1076 (“The Commission has . . . never relied on [this factor] as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the [other] two.”). And finally, the Commission explained that “[u]njustified consumer injury is the primary focus of the FTC Act” and that such an injury “[b]y itself . . . can be sufficient to warrant a finding of unfairness.” 1980 Policy Statement, *supra* at 1073. This “does not mean that every consumer injury is legally ‘unfair.’” *Id.* Indeed,

[t]o justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.

*Id.*

In 1994, Congress codified the 1980 Policy Statement at 15 U.S.C. § 45(n):

The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695. Like the 1980 Policy Statement, § 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.

### *B. Plain Meaning of Unfairness*

Wyndham argues (for the first time on appeal) that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word “unfair” imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair “unless” the act satisfies the three specified requirements, it does not answer whether these are the *only* requirements for a finding of unfairness.) Even if so, some of Wyndham’s proposed requirements are unpersuasive, and the rest are satisfied by the allegations in the FTC’s complaint.

First, citing *FTC v. R.F. Keppel & Brother, Inc.*, 291 U.S. 304 (1934), Wyndham argues that conduct is only unfair when it injures consumers “through unscrupulous or unethical behavior.” Wyndham Br. at 20–21. But *Keppel* nowhere says that unfair conduct must be unscrupulous or unethical. Moreover, in *Sperry* the Supreme Court rejected the view that the FTC’s 1964 policy statement required unfair conduct to be “unscrupulous” or “unethical.” 405 U.S. at 244 n.5.<sup>3</sup>

---

<sup>3</sup> *Id.* (“[Petitioner] argues that . . . [the 1964 statement] commits the FTC to the view that misconduct in respect of the third of these criteria is not subject to constraint as ‘unfair’ absent a concomitant showing of misconduct according to the first or second of these criteria. But all the FTC said in the [1964] statement . . . was that ‘[t]he wide variety of decisions interpreting the elusive concept of unfairness *at least* makes clear that a method of selling violates Section 5 if it is exploitive or inequitable and if, in addition to being morally objectionable, it is seriously



Wyndham points to no subsequent FTC policy statements, adjudications, judicial opinions, or statutes that would suggest any change since *Sperry*.

Next, citing one dictionary, Wyndham argues that a practice is only “unfair” if it is “not equitable” or is “marked by injustice, partiality, or deception.” Wyndham Br. at 18–19 (citing *Webster’s Ninth New Collegiate Dictionary* (1988)). Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

We recognize this analysis of unfairness encompasses some facts relevant to the FTC’s deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. *See, e.g., Am. Fin. Servs. Ass’n v. FTC*, 767 F.2d 957, 980 n.27 (D.C. Cir. 1985) (“The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice.”); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1367 (11th Cir. 1988) (“[A] practice may be both deceptive and unfair . . .”).<sup>4</sup> We cannot completely disentangle the two

---

detrimental to consumers or others.” (emphasis and some alterations in original, citation omitted)).

<sup>4</sup> The FTC has on occasion described deception as a subset of unfairness. *See Int’l Harvester Co.*, 104 F.T.C. at 1060 (“The Commission’s unfairness jurisdiction provides a more general basis for action against acts or practices which cause significant consumer injury. This part of our jurisdiction is

theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a

---

broader than that involving deception, and the standards for its exercise are correspondingly more stringent. . . . [U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset.”); *Figgie Int’l*, 107 F.T.C. 313, 373 n.5 (1986) (“[U]nfair practices are not always deceptive but deceptive practices are always unfair.”); *Orkin Exterminating Co.*, 108 F.T.C. 263, 363 n.78 (1986). So have several FTC staff members. See, e.g., J. Howard Beales, Director of the Bureau of Consumer Protection, FTC, Marketing and Public Policy Conference, The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) (“Although, in the past, they have sometimes been viewed as mutually exclusive legal theories, Commission precedent incorporated in the statutory codification makes clear that deception is properly viewed as a subset of unfairness.”); Neil W. Averitt, *The Meaning of “Unfair Acts or Practices” in Section 5 of the Federal Trade Commission Act*, 70 Geo. L.J. 225, 265–66 (1981) (“Although deception is generally regarded as a separate aspect of section 5, in its underlying rationale it is really just one specific form of unfair consumer practice . . . . [For example, the] Commission has held that it is deceptive for a merchant to make an advertising claim for which he lacks a reasonable basis, regardless of whether the claim is eventually proven true or false . . . . Precisely because unsubstantiated ads are deceptive in this manner, . . . they also affect the exercise of consumer sovereignty and thus constitute an unfair act or practice.”).

misleading privacy policy that overstated its cybersecurity. Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant at 5, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887) ("Consumers could not take steps to avoid Wyndham's unreasonable data security [before providing their personal information] because Wyndham falsely told consumers that it followed 'industry standard practices.'"); see JA 203 ("On the reasonable avoidable part, . . . consumers certainly would not have known that Wyndham had unreasonable data security practices in this case . . . . We also allege that in [Wyndham's] privacy policy they deceive consumers by saying we do have reasonable security data practices. That is one way consumers couldn't possibly have avoided providing a credit card to a company."). Wyndham did not challenge this argument in the District Court nor does it do so now. If Wyndham's conduct satisfies the reasonably avoidable requirement at least partially because of its privacy policy—an inference we find plausible at this stage of the litigation—then the policy is directly relevant to whether Wyndham's conduct was unfair.<sup>5</sup>

Continuing on, Wyndham asserts that a business “does not treat its customers in an ‘unfair’ manner when the business *itself* is victimized by criminals.” Wyndham Br. at

---

<sup>5</sup> No doubt there is an argument that consumers could not reasonably avoid injury even absent the misleading privacy policy. See, e.g., James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. Ill. J.L. Tech. & Pol'y. 1 (arguing that consumers may care about data privacy, but be unable to consider it when making credit card purchases). We have no occasion to reach this question, as the parties have not raised it.

21 (emphasis in original). It offers no reasoning or authority for this principle, and we can think of none ourselves. Although unfairness claims “usually involve actual and completed harms,” *Int’l Harvester*, 104 F.T.C. at 1061, “they may also be brought on the basis of likely rather than actual injury,” *id.* at 1061 n.45. And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. 15 U.S.C. § 45(n) (“[An unfair act or practice] causes or is *likely to cause* substantial injury” (emphasis added)). More importantly, that a company’s conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms. See Restatement (Second) of Torts § 449 (1965) (“If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby.”); *Westfarm Assocs. v. Wash. Suburban Sanitary Comm’n*, 66 F.3d 669, 688 (4th Cir. 1995) (“Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable.”). For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks.

Finally, Wyndham posits a *reductio ad absurdum*, arguing that if the FTC’s unfairness authority extends to Wyndham’s conduct, then the FTC also has the authority to “regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door,” Wyndham Br. at 23, and to sue supermarkets that are “sloppy about sweeping up banana peels,” Wyndham Reply Br. at 6. The argument is alarmist to say the least. And it invites the

tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair."

### *C. Subsequent Congressional Action*

Wyndham next argues that, even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data. *See* Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 1985-86 (2003) (codified as amended at 15 U.S.C. § 1681w). The Gramm-Leach-Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436-37 (1999) (codified as amended at 15 U.S.C. § 6801(b)). And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . . , how the operator uses such information, and the operator's disclosure practices for such information." Pub. L. No. 105-277, § 1303, 112 Stat. 2681, 2681-730-732 (1998) (codified as amended at 15 U.S.C. § 6502).<sup>6</sup> Wyndham contends these "tailored grants of

---

<sup>6</sup> Wyndham also points to a variety of cybersecurity bills that Congress has considered and not passed. "[S]ubsequent legislative history . . . is particularly dangerous ground on

substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field.” Wyndham Br. at 25. Citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000), Wyndham concludes that Congress excluded cybersecurity from the FTC’s unfairness authority by enacting these measures.

We are not persuaded. The inference to congressional intent based on post-enactment legislative activity in *Brown & Williamson* was far stronger. There, the Food and Drug Administration had repeatedly disclaimed regulatory authority over tobacco products for decades. *Id.* at 144. During that period, Congress enacted six statutes regulating tobacco. *Id.* at 143–44. The FDA later shifted its position, claiming authority over tobacco products. The Supreme Court held that Congress excluded tobacco-related products from the FDA’s authority in enacting the statutes. As tobacco products would necessarily be banned if subject to the FDA’s regulatory authority, any interpretation to the contrary would contradict congressional intent to regulate rather than ban tobacco products outright. *Id.* 137–39; *Massachusetts v. EPA*, 549 U.S. 497, 530–31 (2007). Wyndham does not argue that recent privacy laws *contradict* reading corporate cybersecurity into § 45(a). Instead, it merely asserts that Congress had no reason to enact them if the FTC could already regulate cybersecurity through that provision. Wyndham Br. at 25–26.

We disagree that Congress lacked reason to pass the recent legislation if the FTC already had regulatory authority over some cybersecurity issues. The Fair Credit Reporting

---

which to rest an interpretation of a prior statute when it concerns . . . a proposal that does not become law.” *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990).

Act requires (rather than authorizes) the FTC to issue regulations, 15 U.S.C. § 1681w (“The Federal Trade Commission . . . *shall* issue final regulations requiring . . .” (emphasis added)); *id.* § 1681m(e)(1)(B) (“The [FTC and other agencies] *shall* jointly . . . prescribe regulations requiring each financial institution . . .” (emphasis added)), and expands the scope of the FTC’s authority, *id.* § 1681s(a)(1) (“[A] violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce . . . and shall be subject to enforcement by the [FTC] . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act.”). The Gramm-Leach-Bliley Act similarly requires the FTC to promulgate regulations, *id.* § 6801(b) (“[The FTC] shall establish appropriate standards for the financial institutions subject to [its] jurisdiction . . .”), and relieves some of the burdensome § 45(n) requirements for declaring acts unfair, *id.* § 6801(b) (“[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer.*” (emphasis added)). And the Children’s Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, *id.* § 6502(b) (citing 5 U.S.C. § 553), rather than the more burdensome Magnuson-Moss procedures under which the FTC must usually issue regulations, 15 U.S.C. § 57a. Thus none of the recent privacy legislation was “inexplicable” if the FTC already had some authority to regulate corporate cybersecurity through § 45(a).

Next, Wyndham claims that the FTC’s interpretation of § 45(a) is “inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here.” Wyndham Br. at 28. Yet again we disagree. In two of the

statements cited by Wyndham, the FTC clearly said that some cybersecurity practices are “unfair” under the statute. *See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 2358081, at \*6 (June 15, 2011) (statement of Edith Ramirez, Comm’r, FTC) (“[T]he Commission enforces the FTC Act’s proscription against unfair . . . acts . . . in cases where a business[’s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.”); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 1971214, at \*7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

In the two other cited statements, given in 1998 and 2000, the FTC only acknowledged that it cannot require companies to adopt “fair information practice policies.” *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 34 (2000) [hereinafter *Privacy Online*]; *Privacy in Cyberspace: Hearing Before the Subcomm. on Telecomms., Trade & Consumer Prot. of the H. Comm. on Commerce*, 1998 WL 546441 (July 21, 1998) (statement of Robert Pitofsky, Chairman, FTC). These policies would protect consumers from far more than the kind of “substantial injury” typically covered by § 45(a). In addition to imposing some cybersecurity requirements, they would require companies to give notice about what data they collect from consumers, to permit those consumers to decide how the data is used, and to permit them to review and correct inaccuracies. *Privacy Online*, *supra* at 36–37. As the FTC explained in the District Court, the primary concern driving the adoption of these policies in the late 1990s was that “companies . . . were capable of *collecting* enormous amounts of information about consumers, and people were suddenly realizing this.” JA 106 (emphasis added). The FTC



thus could not require companies to adopt broad fair information practice policies because they were “just collecting th[e] information, and consumers [were not] injured.” *Id.*; *see also* Order Denying Respondent LabMD’s Motion to Dismiss, No. 9357, slip op. at 7 (Jan. 16, 2014) [hereinafter *LabMD Order* or *LabMD*] (“[T]he sentences from the 1998 and 2000 reports . . . simply recognize that the Commission’s existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children’s online privacy) . . . .” (emphasis in original)). Our conclusion is this: that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency’s earlier position.

Having rejected Wyndham’s arguments that its conduct cannot be unfair, we assume for the remainder of this opinion that it was.

#### **IV. Fair Notice**

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained “fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.” *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (internal quotation marks omitted). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a),

the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.<sup>7</sup>

#### *A. Legal Standard*

The level of required notice for a person to be subject to liability varies by circumstance. In *Bouie v. City of Columbia*, the Supreme Court held that a “judicial construction of a criminal statute” violates due process if it is “unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue.” 378 U.S. 347, 354 (1964) (internal quotation marks omitted); *see also* *Rogers v. Tennessee*, 532 U.S. 451, 457 (2001); *In re Surrick*, 338 F.3d 224, 233–34 (3d Cir. 2003). The precise meaning of “unexpected and indefensible” is not entirely clear, *United States v. Lata*, 415 F.3d 107, 111 (1st Cir. 2005), but we and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute.<sup>8</sup>

---

<sup>7</sup> We do not read Wyndham’s briefing as raising a meaningful argument under the “discriminatory enforcement” prong. A few sentences in a reply brief are not enough. *See* Wyndham Reply Br. at 26 (“To provide the notice required by due process, a statement must in some sense declare what conduct the law proscribes and thereby constrain enforcement discretion . . . . Here, the consent decrees at issue . . . do not limit the Commission’s enforcement authority in any way.” (citation omitted)).

<sup>8</sup> *See Ortiz v. N.Y.S. Parole*, 586 F.3d 149, 159 (2d Cir. 2009) (holding that the “unexpected and indefensible” standard “requires only that the law . . . not lull the potential defendant

The fair notice doctrine extends to civil cases, particularly where a penalty is imposed. *See Fox Television Stations, Inc.*, 132 S. Ct. at 2317–20; *Boutilier v. INS*, 387 U.S. 118, 123 (1967). “Lesser degrees of specificity” are allowed in civil cases because the consequences are smaller than in the criminal context. *San Filippo v. Bongiovanni*, 961 F.2d 1125, 1135 (3d Cir. 1992). The standards are especially lax for civil statutes that regulate economic activities. For those statutes, a party lacks fair notice when the relevant standard is “so vague as to be no rule or standard at all.”

---

into a *false sense of security*, giving him *no reason even to suspect* that his conduct *might* be within its scope.” (emphases added)); *In re Surrick*, 338 F.3d at 234 (“[We] reject [the] contention that . . . nothing in the history of [the relevant provision] had stated *or even foreshadowed* that reckless conduct *could* violate it. Indeed, in view of the foregoing, the [state court’s] decision . . . was neither ‘unexpected’ nor ‘indefensible’ by reference to the law which had been expressed prior to the conduct in issue.” (emphases added)); *Warner v. Zent*, 997 F.2d 116, 125 (6th Cir. 1993) (“‘The underlying principle is that no man shall be held criminally responsible for conduct which *he could not reasonably understand* to be proscribed.’” (emphasis added) (quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954))); *id.* at 127 (“It was *by no means unforeseeable* . . . that the [court] would [construe the statute as it did].” (emphasis added)); *see also Lata*, 415 F.3d at 112 (“[S]omeone in [the defendant’s] position *could not reasonably be surprised* by the sentence he eventually received . . . . We reserve for the future the case . . . in which a sentence is imposed . . . that is *higher than any that might realistically have been imagined* at the time of the crime . . . .” (emphases added)).

*CMR D.N. Corp. v. City of Phila.*, 703 F.3d 612, 631–32 (3d Cir. 2013) (internal quotation marks omitted).<sup>9</sup>

A different set of considerations is implicated when agencies are involved in statutory or regulatory interpretation. Broadly speaking, agencies interpret in at least three contexts. One is where an agency administers a statute without any special authority to create new rights or obligations. When disputes arise under this kind of agency interpretation, the courts give respect to the agency’s view to the extent it is persuasive, but they retain the primary responsibility for construing the statute.<sup>10</sup> As such, the

---

<sup>9</sup> See also *Bongiovanni*, 961 F.2d at 1138; *Boutilier*, 387 U.S. at 123; *Leib v. Hillsborough Cnty. Pub. Transp. Comm’n*, 558 F.3d 1301, 1310 (11th Cir. 2009); *Ford Motor Co. v. Tex. Dep’t of Transp.*, 264 F.3d 493, 507 (5th Cir. 2001); *Columbia Nat’l Res., Inc. v. Tatum*, 58 F.3d 1101, 1108 (6th Cir. 1995).

<sup>10</sup> See *Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944) (“[The agency interpretation is] not controlling upon the courts by reason of [its] authority [but is a] body of experience and informed judgment to which courts . . . may properly resort for guidance.”); *Christenson v. Harris Cnty.*, 529 U.S. 576, 587 (2000) (“[Agency interpretations are] entitled to respect under [*Skidmore*], but only to the extent that [they] have the power to persuade.” (internal quotation marks omitted)); see also Peter L. Strauss, “*Deference*” is Too Confusing—Let’s Call Them “Chevron Space” and “Skidmore Weight”, 112 Colum. L. Rev. 1143, 1147 (2012) (“*Skidmore* . . . is grounded in a construct of the agency as responsible expert, arguably possessing special knowledge of

standard of notice afforded to litigants about the meaning of the statute is not dissimilar to the standard of notice for civil statutes generally because the court, not the agency, is the ultimate arbiter of the statute's meaning.

The second context is where an agency exercises its authority to fill gaps in a statutory scheme. There the agency is primarily responsible for interpreting the statute because the courts must defer to any reasonable construction it adopts. *See Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984). Courts appear to apply a more stringent standard of notice to civil regulations than civil statutes: parties are entitled to have “ascertainable certainty” of what conduct is legally required by the regulation. *See Chem. Waste Mgmt., Inc. v. EPA*, 976 F.2d 2, 29 (D.C. Cir. 1992) (*per curiam*) (denying petitioners’ challenge that a recently promulgated EPA regulation fails fair notice principles); *Nat’l Oilseed Processors Ass’n. v. OSHA*, 769 F.3d 1173, 1183–84 (D.C. Cir. 2014) (denying petitioners’ challenge that a recently promulgated OSHA regulation fails fair notice principles).

The third context is where an agency interprets the meaning of its own regulation. Here also courts typically must defer to the agency’s reasonable interpretation.<sup>11</sup> We

---

the statutory meaning a court should consider in *reaching its own judgment*.” (emphasis added)).

<sup>11</sup> *See Auer v. Robbins*, 519 U.S. 452, 461 (1997) (“Because the salary-basis test is a creature of the Secretary’s own regulations, his interpretation of it is . . . controlling unless plainly erroneous or inconsistent with the regulation.” (internal quotation marks omitted)); *Decker v. Nw. Env’tl. Def. Ctr.*, 133 S. Ct. 1326, 1337 (2013) (“When an agency

and several of our sister circuits have stated that private parties are entitled to know with “ascertainable certainty” an agency’s interpretation of its regulation. *Sec’y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008); *Dravo Corp. v. Occupational Safety & Health Rev. Comm’n*, 613 F.2d 1227, 1232–33 (3d Cir. 1980).<sup>12</sup> Indeed,

---

interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation.” (internal quotation marks omitted)); *Martin v. Occupational Safety & Health Rev. Comm’n*, 499 U.S. 144, 150–51 (1991) (“In situations in which the meaning of [regulatory] language is not free from doubt, the reviewing court should give effect to the agency’s interpretation so long as it is reasonable.” (alterations in original, internal quotations omitted)); *Columbia Gas Transp., LLC v. 1.01 Acres, More or Less in Penn Twp.*, 768 F.3d 300, 313 (3d Cir. 2014) (“[A]s an agency interpretation of its own regulation, it is deserving of deference.” (citing *Decker*)).

<sup>12</sup> See also *Wis. Res. Prot. Council v. Flambeau Mining Co.*, 727 F.3d 700, 708 (7th Cir. 2013); *AJP Const., Inc. v. Sec’y of Labor*, 357 F.3d 70, 75–76 (D.C. Cir. 2004) (quoting *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995)); *Tex. Mun. Power Agency v. EPA*, 89 F.3d 858, 872 (D.C. Cir. 1996); *Ga. Pac. Corp. v. Occupational Safety & Health Rev. Comm’n*, 25 F.3d 999, 1005 (11th Cir. 1994); *Diamond Roofing Co. v. Occupational Safety & Health Rev. Comm’n*, 528 F.2d 645, 649 (5th Cir. 1976). In fact, the Supreme Court applied *Skidmore* to an interpretation by an agency of a regulation it adopted instead of deferring to that interpretation because the latter would have “seriously undermine[d] the principle that agencies should provide regulated parties fair

“the due process clause prevents . . . deference from validating the application of a regulation that fails to give fair warning of the conduct it prohibits or requires.” *AJP Const., Inc.*, 357 F.3d at 75 (internal quotation marks omitted).

A higher standard of fair notice applies in the second and third contexts than in the typical civil statutory interpretation case because agencies engage in interpretation differently than courts. See Frank H. Easterbook, *Judicial Discretion in Statutory Interpretation*, 57 Okla. L. Rev. 1, 3 (2004) (“A judge who announces deference is approving a shift in interpretive method, not just a shift in the identity of the decider, as if a suit were being transferred to a court in a different venue.”). In resolving ambiguity in statutes or regulations, courts generally adopt the *best* or *most reasonable* interpretation. But, as the agency is often free to adopt *any reasonable construction*, it may impose higher legal obligations than required by the best interpretation.<sup>13</sup>

---

warning of the conduct [a regulation] prohibits or requires.” *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 & n.15 (2012) (second alteration in original, internal quotation marks omitted) (citing *Dravo*, 613 F.2d at 1232–33 and the “ascertainable certainty” standard).

<sup>13</sup> See *Nat’l Cable & Telecomms. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 980 (2005) (“If a statute is ambiguous, and if the implementing agency’s construction is reasonable, *Chevron* requires a federal court to accept the agency’s construction of the statute, even if the agency’s reading differs from what the court believes is the best statutory interpretation.”); *Decker*, 133 S. Ct. at 1337 (“It is well established that an agency’s interpretation need not be the only possible reading of a regulation—or even the best one—

Furthermore, courts generally resolve statutory ambiguity by applying traditional methods of construction. Private parties can reliably predict the court's interpretation by applying the same methods. In contrast, an agency may also rely on technical expertise and political values.<sup>14</sup> It is harder to predict how an agency will construe a statute or regulation at some unspecified point in the future, particularly when that interpretation will depend on the "political views of

---

to prevail. When an agency interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation." (internal quotation marks omitted)); *Auer*, 519 U.S. at 462–63 ("[The rule that Fair Labor Standards Act] exemptions are to be narrowly construed against . . . employers . . . is a rule governing judicial interpretation of statutes and regulations, not a limitation on the Secretary's power to resolve ambiguities in his own regulations. A rule requiring the Secretary to construe his own regulations narrowly would make little sense, since he is free to write the regulations as broadly as he wishes, subject only to the limits imposed by the statute." (internal quotation marks omitted)).

<sup>14</sup> See *Garfias-Rodriguez v. Holder*, 702 F.3d 504, 518 (9th Cir. 2012) (rejecting the applicability of the judicial retroactivity test to a new Board of Immigration Appeals' interpretation because the "decision fill[ed] a statutory gap and [was] an exercise [of the agency's] policymaking function"); Easterbrook, *supra* at 3 ("Judges in their own work forswear the methods that agencies employ" to interpret statutes, which include relying on "political pressure, the President's view of happy outcomes, cost-benefit studies . . . and the other tools of policy wonks . . .").



the President in office at [that] time.” Strauss, *supra* at 1147.<sup>15</sup>

Wyndham argues it was entitled to “ascertainable certainty” of the FTC’s interpretation of what specific cybersecurity practices are required by § 45(a). Yet it has contended repeatedly—no less than seven separate occasions in *this* case—that there is no FTC rule or adjudication about cybersecurity that merits deference here. The necessary implication, one that Wyndham itself has explicitly drawn on two occasions noted below, is that federal courts are to interpret § 45(a) in the first instance to decide whether Wyndham’s conduct was unfair.

Wyndham’s argument has focused on the FTC’s motion to dismiss order in *LabMD*, an administrative case in which the agency is pursuing an unfairness claim based on allegedly inadequate cybersecurity. *LabMD Order, supra*. Wyndham first argued in the District Court that the *LabMD Order* does not merit *Chevron* deference because “self-serving, litigation-driven decisions . . . are entitled to no deference at all” and because the opinion adopted an impermissible construction of the statute. Wyndham’s

---

<sup>15</sup> See also *Brand X Internet Servs.*, 545 U.S. at 981 (“[T]he agency . . . must consider varying interpretations and the wisdom of its policy on a continuing basis . . . in response to . . . a change in administrations.” (internal quotation marks omitted, first omission in original)); *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 59 (1983) (Rehnquist, J., dissenting in part) (“A change in administration brought about by the people casting their votes is a perfectly reasonable basis for an executive agency’s reappraisal of the costs and benefits of its . . . regulations.”).

January 29, 2014 Letter at 1–2, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887).

Second, Wyndham switched gears in its opening brief on appeal to us, arguing that *LabMD* does not merit *Chevron* deference because courts owe no deference to an agency’s interpretation of the “boundaries of Congress’ statutory delegation of authority to the agency.” Wyndham Br. at 19–20.

Third, in its reply brief it argued again that *LabMD* does not merit *Chevron* deference because it adopted an impermissible construction of the statute. Wyndham Reply Br. at 14.

Fourth, Wyndham switched gears once more in a Rule 28(j) letter, arguing that *LabMD* does not merit *Chevron* deference because the decision was nonfinal. Wyndham’s February 6, 2015 Letter (citing *LabMD, Inc. v. FTC*, 776 F.3d 1275 (11th Cir. 2015)).

Fifth, at oral argument we asked Wyndham whether the FTC has decided that cybersecurity practices are unfair. Counsel answered: “No. I don’t think consent decrees count, I don’t think the 2007 brochure counts, and I don’t think *Chevron* deference applies. So are . . . they asking this federal court in the first instance . . . [?] I think the answer to that question is yes . . . .” Oral Arg. Tr. at 19.

Sixth, due to our continuing confusion about the parties’ positions on a number of issues in the case, we asked for supplemental briefing on certain questions, including whether the FTC had declared that cybersecurity practices can be unfair. In response, Wyndham asserted that “the FTC has not declared unreasonable cybersecurity practices ‘unfair.’” Wyndham’s Supp. Memo. at 3. Wyndham

explained further: “It follows from [our] answer to [that] question that the FTC is asking the federal courts to determine in the first instance that unreasonable cybersecurity practices qualify as ‘unfair’ trade practices under the FTC Act.” *Id.* at 4.

Seventh, and most recently, Wyndham submitted a Rule 28(j) letter arguing that *LabMD* does not merit *Chevron* deference because it decided a question of “deep economic and political significance.” Wyndham’s June 30, 2015 Letter (quoting *King v. Burwell*, 135 S. Ct. 2480 (2015)).

Wyndham’s position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham’s conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the *FTC’s interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires.

Indeed, at oral argument we asked Wyndham whether the cases cited in its brief that apply the “ascertainable certainty” standard—all of which involve a court reviewing an agency adjudication<sup>16</sup> or at least a court being asked to

---

<sup>16</sup> See *Fox Television Stations, Inc.*, 132 S. Ct. 2307 (vacating an FCC adjudication for lack of fair notice of an agency interpretation); *PMD Produce Brokerage Corp. v. USDA*, 234

defer to an agency interpretation<sup>17</sup>—apply where the court is to decide the meaning of the statute in the first instance.<sup>18</sup> Wyndham’s counsel responded, “I think it would, your Honor. I think if you go to *Ford Motor* [*Co. v. FTC*, 673 F.2d 1008 (9th Cir. 1981)], I think that’s what was happening there.” Oral Arg. Tr. at 61. But *Ford Motor* is readily distinguishable. Unlike Wyndham, the petitioners there did not bring a fair notice claim under the Due Process Clause. Instead, they argued that, per *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974), the FTC abused its discretion by proceeding through agency adjudication rather than

---

F.3d 48 (D.C. Cir. 2000) (vacating the dismissal of an administrative appeal issued by a Judicial Officer in the Department of Agriculture because the agency’s Rules of Practice failed to give fair notice of the deadline for filing an appeal); *Gen. Elec. Co.*, 53 F.3d 1324 (vacating an EPA adjudication for lack of fair notice of the agency’s interpretation of a regulation); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374 (1965) (reviewing an FTC adjudication that found liability).

<sup>17</sup> See *In re Metro-East Mfg. Co.*, 655 F.2d 805, 810–12 (7th Cir. 1981) (declining to defer to an agency’s interpretation of its own regulation because the defendant could not have known with ascertainable certainty the agency’s interpretation).

<sup>18</sup> We asked, “All of your cases on fair notice pertain to an agency’s *interpretation* of its own regulation or the statute that governs that agency. Does this fair notice doctrine apply where it is a court announcing an *interpretation* of a statute in the first instance?” Oral Arg. Tr. at 60 (emphases added).

rulemaking.<sup>19</sup> More importantly, the Ninth Circuit was reviewing an agency adjudication; it was not interpreting the meaning of the FTC Act in the first instance.

In addition, our understanding of Wyndham's position is consistent with the District Court's opinion, which concluded that the FTC has stated a claim under § 45(a) based on the Court's interpretation of the statute and without any reference to *LabMD* or any other agency adjudication or

---

<sup>19</sup> To the extent Wyndham could have raised this argument, we do not read its briefs to do so. Indeed, its opening brief appears to repudiate the theory. Wyndham Br. at 38–39 (“The district court below framed the fair notice issue here as whether ‘the FTC must formally promulgate regulations before bringing its unfairness claim.’ With all respect, that characterization of Wyndham’s position is a straw man. Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication. *See, e.g., [Bell Aerospace Co., 416 U.S. at 290–95]*. Rather, Wyndham’s point is only that, however an agency chooses to proceed, it must provide regulated entities with constitutionally requisite fair notice.” (internal citations omitted)). Moreover, the Supreme Court has explained that where “it is doubtful [that] any generalized standard could be framed which would have more than marginal utility[, the agency] has reason to . . . develop[] its standards in a case-by-case manner.” *Bell Aerospace Co., 416 U.S. at 294*. An agency’s “judgment that adjudication best serves this purpose is entitled to great weight.” *Id.* Wyndham’s opening brief acknowledges that the FTC has given this rationale for proceeding by adjudication, Wyndham Br. at 37–38, but, the company offers no ground to challenge it.

regulation. *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621–26 (D.N.J. 2014).

We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC’s interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham’s liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham’s forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency’s interpretation of the statute.

*B. Did Wyndham Have Fair Notice of the Meaning of § 45(a)?*

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham’s briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham’s briefing focuses on the FTC’s failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100-

year-old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

Moreover, Wyndham is entitled to a relatively low level of statutory notice for several reasons. Subsection 45(a) does not implicate any constitutional rights here. *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982). It is a civil rather than criminal statute.<sup>20</sup> *Id.* at 498–99. And statutes regulating economic activity receive a “less strict” test because their “subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action.” *Id.* at 498.

In this context, the relevant legal rule is not “so vague as to be ‘no rule or standard at all.’” *CMR D.N. Corp.*, 703 F.3d at 632 (quoting *Boutilier*, 387 U.S. at 123). Subsection 45(n) asks whether “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, *Pa. Funeral Dirs. Ass’n v. FTC*, 41 F.3d 81, 89–92 (3d Cir. 1992); *Am. Fin. Servs. Ass’n*, 767 F.2d at 975, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that

---

<sup>20</sup> While civil statutes containing “quasi-criminal penalties may be subject to the more stringent review afforded criminal statutes,” *Ford Motor Co.*, 264 F.3d at 508, we do not know what remedy, if any, the District Court will impose. And Wyndham’s briefing does not indicate what kinds of remedies it is exposed to in this proceeding.

would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. *Cf. Nash v. United States*, 229 U.S. 373, 377 (1913) (“[T]he law is full of instances where a man’s fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree.”). Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.

What appears to us is that Wyndham’s fair notice claim must be reviewed as an as-applied challenge. *See United States v. Mazurie*, 419 U.S. 544, 550 (1975); *San Filippo*, 961 F.2d at 1136. Yet Wyndham does not argue that its cybersecurity practices survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). One sentence in Wyndham’s reply brief says that its “view of what data-security practices are unreasonable . . . is not necessarily the same as the FTC’s.” Wyndham Reply Br. at 23. Too little and too late.

Wyndham’s as-applied challenge falls well short given the allegations in the FTC’s complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, Compl. at ¶ 24(a), did not restrict specific IP addresses *at all*, *id.* at ¶ 24(j), did not use *any* encryption for certain customer files, *id.* at ¶ 24(b), and did not require some users to change their default or factory-setting passwords *at all*, *id.* at ¶ 24(f). Wyndham did not respond to this argument in its reply brief.



Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham's fair notice challenge fails. In 2007 the FTC issued a guidebook, *Protecting Personal Information: A Guide for Business*, FTC Response Br. Attachment 1 [hereinafter *FTC Guidebook*], which describes a "checklist[]" of practices that form a "sound data security plan." *Id.* at 3. The guidebook does not state that any particular practice is required by § 45(a),<sup>21</sup> but it does counsel against many of the specific practices alleged here. For instance, it recommends that companies "consider encrypting sensitive information that is stored on [a] computer network . . . [, c]heck . . . software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." *Id.* at 10. It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through

---

<sup>21</sup> For this reason, we agree with Wyndham that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question.

the firewall and what they will be allowed to see . . . to allow only trusted employees with a legitimate business need to access the network.” *Id.* at 14. It recommends “requiring that employees use ‘strong’ passwords” and cautions that “[h]ackers will first try words like . . . the software’s default password[] and other easy-to-guess choices.” *Id.* at 12. And it recommends implementing a “breach response plan,” *id.* at 16, which includes “[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information,” *id.* at 23.

As the agency responsible for administering the statute, the FTC’s expert views about the characteristics of a “sound data security plan” could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. FTC Br. at 47 n.16. The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not “adjudications on the merits.”<sup>22</sup> Wyndham Br. at 41. But even where the “ascertainable certainty” standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor “adjudications on the merits.” *See, e.g., United States v.*

---

<sup>22</sup> We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).

*Lachman*, 387 F.3d 42, 57 (1st Cir. 2004) (noting that fair notice principles can be satisfied even where a regulation is vague if the agency “provide[d] a sufficient, publicly accessible statement” of the agency’s interpretation of the regulation); *Beverly Healthcare-Hillview*, 541 F.3d at 202 (citing *Lachman* and treating an OSHA opinion letter as a “sufficient, publicly accessible statement”); *Gen. Elec. Co.*, 53 F.3d at 1329. That the FTC commissioners—who must vote on whether to issue a complaint, 16 C.F.R. § 3.11(a); ABA Section of Antitrust Law, *FTC Practice and Procedure Manual* 160–61 (2007)—believe that alleged cybersecurity practices fail the cost-benefit analysis of § 45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well.<sup>23</sup>

---

<sup>23</sup> We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC’s only answer was that “if you’re a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things.” Oral Arg. Tr. at 51. We also asked whether the FTC has “informed the public that it needs to look at complaints and consent decrees for guidance,” and the Commission could offer no examples. *Id.* at 52. But Wyndham does not appear to argue it was unaware of the consent decrees and complaints; it claims only that they did not give notice of what the law requires. Wyndham Reply Br. at 25 (“The fact that the FTC publishes these materials on its website and provides notice in the Federal Register, moreover, is immaterial—the problem is not that Wyndham lacked notice *of the consent decrees* [which

Wyndham next contends that the individual allegations in the complaints are too vague to be relevant to the fair notice analysis. Wyndham Br. at 41–42. It does not, however, identify any specific examples. And as the Table below reveals, the individual allegations were specific and similar to those here in at least one of the four or five<sup>24</sup> cybersecurity-related unfair-practice complaints that issued prior to the first attack.

Wyndham also argues that, even if the individual allegations are not vague, the complaints “fail to spell out what specific cybersecurity practices . . . actually triggered the alleged violation, . . . provid[ing] only a . . . description of certain alleged problems that, ‘*taken together*,’” fail the cost-benefit analysis. Wyndham Br. at 42 (emphasis in original). We part with it on two fronts. First, even if the complaints do not specify which allegations, in the Commission’s view, form the necessary and sufficient conditions of the alleged violation, they can still help companies apprehend the possibility of liability under the statute. Second, as the Table below shows, Wyndham cannot argue that the complaints fail to give notice of the necessary and sufficient conditions of an

---

reference the complaints] but that consent decrees [and presumably complaints] by their nature do not give notice *of what Section 5 requires*.” (emphases in original, citations and internal quotations omitted)).

<sup>24</sup> The FTC asserts that five such complaints issued prior to the first attack in April 2008. See FTC Br. at 47–48 n.16. There is some ambiguity, however, about whether one of them issued several months later. See Complaint, *TJX Co.*, No. C-4227 (FTC 2008) (stating that the complaint was issued on July 29, 2008). We note that this complaint also shares significant parallels with the allegations here.

alleged § 45(a) violation when all of the allegations in at least one of the relevant four or five complaints have close corollaries here. *See* Complaint, *CardSystems Solutions, Inc.*, No. C-4168 (FTC 2006) [hereinafter CCS].

**Table: Comparing CSS and Wyndham Complaints**

	CSS	Wyndham
<b>1</b>	Created unnecessary risks to personal information by storing it in a vulnerable format for up to 30 days, CSS at ¶ 6(1).	Allowed software at hotels to store payment card information in clear readable text, Compl. at ¶ 24(b).
<b>2</b>	Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks; did not implement simple, low-cost and readily available defenses to such attacks, CSS at ¶ 6(2)–(3).	Failed to monitor network for the malware used in a previous intrusion, Compl. at ¶ 24(i), which was then reused by hackers later to access the system again, <i>id.</i> at ¶ 34.
<b>3</b>	Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).	Did not employ common methods to require user IDs and passwords that are difficult for hackers to guess. <i>E.g.</i> , allowed remote access to a hotel’s property management system that used default/factory setting passwords, Compl. at ¶ 24(f).

<b>4</b>	Did not use readily available security measures to limit access between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).	Did not use readily available security measures, such as firewalls, to limit access between and among hotels' property management systems, the Wyndham network, and the Internet, Compl. at ¶ 24(a).
<b>5</b>	Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations, CSS at ¶ 6(6).	Failed to employ reasonable measures to detect and prevent unauthorized access to computer network or to conduct security investigations, Compl. at ¶ 24(h).

In sum, we have little trouble rejecting Wyndham's fair notice claim.

## **V. Conclusion**

The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC's claim here. Furthermore, Wyndham repeatedly argued there is no FTC interpretation of § 45(a) or (n) to which the federal courts must defer in this case, and, as a result, the courts must interpret the meaning of the statute as it applies to Wyndham's conduct in the first instance. Thus, Wyndham cannot argue it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statute itself—a

theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

We thus affirm the District Court's decision.

---

**U.S. Department of Health and Human Services  
Office for Civil Rights**



**HIPAA Administrative Simplification**

***Regulation Text***

**45 CFR Parts 160, 162, and 164  
(Unofficial Version, as amended through March 26, 2013)**

---



# HIPAA Administrative Simplification

## Table of Contents

<u>Section</u>	<u>Page</u>
<b>PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS.....</b>	<b>10</b>
<b>SUBPART A—GENERAL PROVISIONS .....</b>	<b>10</b>
§ 160.101 Statutory basis and purpose.....	10
§ 160.102 Applicability.....	11
§ 160.103 Definitions.....	11
§ 160.104 Modifications.....	17
§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.....	17
<b>SUBPART B—PREEMPTION OF STATE LAW .....</b>	<b>17</b>
§ 160.201 Statutory basis.....	17
§ 160.202 Definitions.....	18
§ 160.203 General rule and exceptions.....	18
§ 160.204 Process for requesting exception determinations.....	19
§ 160.205 Duration of effectiveness of exception determinations. ....	19
<b>SUBPART C—COMPLIANCE AND INVESTIGATIONS.....</b>	<b>19</b>
§ 160.300 Applicability.....	19
§ 160.302 [Reserved].....	20
§ 160.304 Principles for achieving compliance.....	20
§ 160.306 Complaints to the Secretary.....	20
§ 160.308 Compliance reviews.....	20
§ 160.310 Responsibilities of covered entities and business associates.....	20

§ 160.312	Secretarial action regarding complaints and compliance reviews.....	21
§ 160.314	Investigational subpoenas and inquiries.....	21
§ 160.316	Refraining from intimidation or retaliation. ....	23
<b>SUBPART D—IMPOSITION OF CIVIL MONEY PENALTIES .....</b>		<b>23</b>
§ 160.400	Applicability.....	23
§ 160.401	Definitions.....	23
§ 160.402	Basis for a civil money penalty. ....	23
§ 160.404	Amount of a civil money penalty. ....	24
§ 160.406	Violations of an identical requirement or prohibition.....	24
§ 160.408	Factors considered in determining the amount of a civil money penalty.....	25
§ 160.410	Affirmative defenses. ....	25
§ 160.412	Waiver.....	26
§ 160.414	Limitations. ....	26
§ 160.416	Authority to settle. ....	26
§ 160.418	Penalty not exclusive.....	26
§ 160.420	Notice of proposed determination. ....	26
§ 160.422	Failure to request a hearing.....	26
§ 160.424	Collection of penalty.....	27
§ 160.426	Notification of the public and other agencies. ....	27
<b>SUBPART E—PROCEDURES FOR HEARINGS .....</b>		<b>27</b>
§ 160.500	Applicability.....	27
§ 160.502	Definitions.....	27
§ 160.504	Hearing before an ALJ.....	27
§ 160.506	Rights of the parties.....	28
§ 160.508	Authority of the ALJ. ....	28
§ 160.510	Ex parte contacts.....	29
§ 160.512	Prehearing conferences. ....	29
§ 160.514	Authority to settle. ....	29

§ 160.516	Discovery. ....	29
§ 160.518	Exchange of witness lists, witness statements, and exhibits. ....	30
§ 160.520	Subpoenas for attendance at hearing. ....	30
§ 160.522	Fees.....	31
§ 160.524	Form, filing, and service of papers. ....	31
§ 160.526	Computation of time. ....	31
§ 160.528	Motions. ....	31
§ 160.530	Sanctions.....	32
§ 160.532	Collateral estoppel. ....	32
§ 160.534	The hearing. ....	32
§ 160.536	Statistical sampling. ....	33
§ 160.538	Witnesses. ....	33
§ 160.540	Evidence.....	33
§ 160.542	The record. ....	34
§ 160.544	Post hearing briefs. ....	34
§ 160.546	ALJ's decision. ....	34
§ 160.548	Appeal of the ALJ's decision.....	34
§ 160.550	Stay of the Secretary's decision. ....	35
 <b>PART 162—ADMINISTRATIVE REQUIREMENTS .....</b>		<b>37</b>
 <b>SUBPART A—GENERAL PROVISIONS .....</b>		<b>38</b>
§ 162.100	Applicability. ....	38
§ 162.103	Definitions.....	38
 <b>SUBPARTS B-C [RESERVED] .....</b>		<b>39</b>
 <b>SUBPART D—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH CARE PROVIDERS.....</b>		<b>39</b>
§ 162.402	[Reserved].....	39

§ 162.404	Compliance dates of the implementation of the standard unique health identifier for health care providers. ....	39
§ 162.406	Standard unique health identifier for health care providers. ....	39
§ 162.408	National Provider System. ....	39
§ 162.410	Implementation specifications: Health care providers. ....	40
§ 162.412	Implementation specifications: Health plans. ....	40
§ 162.414	Implementation specifications: Health care clearinghouses. ....	40
<b>SUBPART E—STANDARD UNIQUE HEALTH IDENTIFIER FOR HEALTH PLANS</b>		<b>40</b>
§ 162.502	[Reserved].....	40
§ 162.504	Compliance requirements for the implementation of the standard unique health plan identifier.....	40
§ 162.506	Standard unique health plan identifier.....	41
§ 162.508	Enumeration System.....	41
§ 162.510	Full implementation requirements: Covered entities. ....	41
§ 162.512	Implementation specifications: Health plans. ....	41
§ 162.514	Other entity identifier.....	42
<b>SUBPART F—STANDARD UNIQUE EMPLOYER IDENTIFIER</b>		<b>42</b>
§ 162.600	Compliance dates of the implementation of the standard unique employer identifier.....	42
§ 162.605	Standard unique employer identifier. ....	42
§ 162.610	Implementation specifications for covered entities.....	42
<b>SUBPARTS G-H [RESERVED]</b> .....		<b>42</b>
<b>SUBPART I—GENERAL PROVISIONS FOR TRANSACTIONS</b>		<b>42</b>
§ 162.900	[Reserved].....	42
§ 162.910	Maintenance of standards and adoption of modifications and new standards. ....	42
§ 162.915	Trading partner agreements.....	43
§ 162.920	Availability of implementation specifications and operating rules.....	43
§ 162.923	Requirements for covered entities. ....	46
§ 162.925	Additional requirements for health plans.....	47

§ 162.930 Additional rules for health care clearinghouses.....	47
§ 162.940 Exceptions from standards to permit testing of proposed modifications.....	48
<b>SUBPART J—CODE SETS.....</b>	<b>49</b>
§ 162.1000 General requirements.....	49
§ 162.1002 Medical data code sets. ....	49
§ 162.1011 Valid code sets.....	50
<b>SUBPART K—HEALTH CARE CLAIMS OR EQUIVALENT ENCOUNTER INFORMATION.....</b>	<b>50</b>
§ 162.1101 Health care claims or equivalent encounter information transaction.....	50
§ 162.1102 Standards for health care claims or equivalent encounter information transaction. ....	50
<b>SUBPART L—ELIGIBILITY FOR A HEALTH PLAN .....</b>	<b>52</b>
§ 162.1201 Eligibility for a health plan transaction. ....	52
§ 162.1202 Standards for eligibility for a health plan transaction. ....	52
§ 162.1203 Operating rules for eligibility for a health plan transaction. ....	52
<b>SUBPART M—REFERRAL CERTIFICATION AND AUTHORIZATION.....</b>	<b>53</b>
§ 162.1301 Referral certification and authorization transaction.....	53
§ 162.1302 Standards for referral certification and authorization transaction. ....	53
<b>SUBPART N—HEALTH CARE CLAIM STATUS .....</b>	<b>54</b>
§ 162.1401 Health care claim status transaction. ....	54
§ 162.1402 Standards for health care claim status transaction. ....	54
§ 162.1403 Operating rules for health care claim status transaction. ....	54
<b>SUBPART O—ENROLLMENT AND DISENROLLMENT IN A HEALTH PLAN .....</b>	<b>54</b>
§ 162.1501 Enrollment and disenrollment in a health plan transaction. ....	54
§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.....	54
<b>SUBPART P—HEALTH CARE ELECTRONIC FUNDS TRANSFERS (EFT) AND REMITTANCE ADVICE .....</b>	<b>55</b>
§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction. ....	55

§ 162.1602	Standards for health care electronic funds transfers (EFT) and remittance advice transaction. ....	55
§ 162.1603	Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction. ....	56
<b>SUBPART Q—HEALTH PLAN PREMIUM PAYMENTS .....</b>		<b>56</b>
§ 162.1701	Health plan premium payments transaction. ....	56
§ 162.1702	Standards for health plan premium payments transaction. ....	56
<b>SUBPART R—COORDINATION OF BENEFITS .....</b>		<b>57</b>
§ 162.1801	Coordination of benefits transaction. ....	57
§ 162.1802	Standards for coordination of benefits information transaction. ....	57
<b>SUBPART S—MEDICAID PHARMACY SUBROGATION.....</b>		<b>58</b>
§ 162.1901	Medicaid pharmacy subrogation transaction.....	58
§ 162.1902	Standard for Medicaid pharmacy subrogation transaction.....	58
 <b>PART 164—SECURITY AND PRIVACY.....</b>		 <b>59</b>
<b>SUBPART A—GENERAL PROVISIONS .....</b>		<b>59</b>
§ 164.102	Statutory basis.....	59
§ 164.103	Definitions.....	59
§ 164.104	Applicability. ....	60
§ 164.105	Organizational requirements.....	60
§ 164.106	Relationship to other parts.....	62
<b>SUBPART B [RESERVED].....</b>		<b>62</b>
 <b>SUBPART C—SECURITY STANDARDS FOR THE PROTECTION OF ELECTRONIC PROTECTED HEALTH INFORMATION.....</b>		 <b>62</b>
§ 164.302	Applicability. ....	62
§ 164.304	Definitions.....	62
§ 164.306	Security standards: General rules. ....	63
§ 164.308	Administrative safeguards. ....	64

§ 164.310 Physical safeguards.....	66
§ 164.312 Technical safeguards. ....	66
§ 164.314 Organizational requirements.....	67
§ 164.316 Policies and procedures and documentation requirements.....	68
§ 164.318 Compliance dates for the initial implementation of the security standards. ....	68
<b>SUBPART D—NOTIFICATION IN THE CASE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION.....</b>	<b>71</b>
§ 164.400 Applicability.....	71
§ 164.402 Definitions.....	71
§ 164.404 Notification to individuals. ....	71
§ 164.406 Notification to the media. ....	72
§ 164.408 Notification to the Secretary. ....	72
§ 164.410 Notification by a business associate.....	73
§ 164.412 Law enforcement delay. ....	73
§ 164.414 Administrative requirements and burden of proof.....	73
<b>SUBPART E—PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.....</b>	<b>73</b>
§ 164.500 Applicability.....	73
§ 164.501 Definitions.....	74
§ 164.502 Uses and disclosures of protected health information: General rules. ....	77
§ 164.504 Uses and disclosures: Organizational requirements.....	81
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations. ....	84
§ 164.508 Uses and disclosures for which an authorization is required. ....	85
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.....	87
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required. ....	88
§ 164.514 Other requirements relating to uses and disclosures of protected health information.....	96
§ 164.520 Notice of privacy practices for protected health information. ....	101
§ 164.522 Rights to request privacy protection for protected health information. ....	104

<b>§ 164.524</b>	<b>Access of individuals to protected health information.....</b>	<b>105</b>
<b>§ 164.526</b>	<b>Amendment of protected health information. ....</b>	<b>108</b>
<b>§ 164.528</b>	<b>Accounting of disclosures of protected health information.....</b>	<b>110</b>
<b>§ 164.530</b>	<b>Administrative requirements.....</b>	<b>111</b>
<b>§ 164.532</b>	<b>Transition provisions.....</b>	<b>114</b>
<b>§ 164.534</b>	<b>Compliance dates for initial implementation of the privacy standards. ....</b>	<b>115</b>



---

## PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

---

### Contents

#### Subpart A—General Provisions

[§ 160.101 Statutory basis and purpose.](#)  
[§ 160.102 Applicability.](#)  
[§ 160.103 Definitions.](#)  
[§ 160.104 Modifications.](#)  
[§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.](#)

#### Subpart B—Preemption of State Law

[§ 160.201 Statutory basis.](#)  
[§ 160.202 Definitions.](#)  
[§ 160.203 General rule and exceptions.](#)  
[§ 160.204 Process for requesting exception determinations.](#)  
[§ 160.205 Duration of effectiveness of exception determinations.](#)

#### Subpart C—Compliance and Investigations

[§ 160.300 Applicability.](#)  
[§ 160.302 \[Reserved\]](#)  
[§ 160.304 Principles for achieving compliance.](#)  
[§ 160.306 Complaints to the Secretary.](#)  
[§ 160.308 Compliance reviews.](#)  
[§ 160.310 Responsibilities of covered entities and business associates.](#)  
[§ 160.312 Secretarial action regarding complaints and compliance reviews.](#)  
[§ 160.314 Investigational subpoenas and inquiries.](#)

[§ 160.316 Refraining from intimidation or retaliation.](#)

#### Subpart D—Imposition of Civil Money Penalties

[§ 160.400 Applicability.](#)  
[§ 160.401 Definitions.](#)  
[§ 160.402 Basis for a civil money penalty.](#)  
[§ 160.404 Amount of a civil money penalty.](#)  
[§ 160.406 Violations of an identical requirement or prohibition.](#)  
[§ 160.408 Factors considered in determining the amount of a civil money penalty.](#)  
[§ 160.410 Affirmative defenses.](#)  
[§ 160.412 Waiver.](#)  
[§ 160.414 Limitations.](#)  
[§ 160.416 Authority to settle.](#)  
[§ 160.418 Penalty not exclusive.](#)  
[§ 160.420 Notice of proposed determination.](#)  
[§ 160.422 Failure to request a hearing.](#)  
[§ 160.424 Collection of penalty.](#)  
[§ 160.426 Notification of the public and other agencies.](#)

#### Subpart E—Procedures for Hearings

[§ 160.500 Applicability.](#)  
[§ 160.502 Definitions.](#)  
[§ 160.504 Hearing before an ALJ.](#)  
[§ 160.506 Rights of the parties.](#)  
[§ 160.508 Authority of the ALJ.](#)  
[§ 160.510 Ex parte contacts.](#)  
[§ 160.512 Prehearing conferences.](#)  
[§ 160.514 Authority to settle.](#)  
[§ 160.516 Discovery.](#)  
[§ 160.518 Exchange of witness lists, witness statements, and exhibits.](#)  
[§ 160.520 Subpoenas for attendance at hearing.](#)

[§ 160.522 Fees.](#)  
[§ 160.524 Form, filing, and service of papers.](#)  
[§ 160.526 Computation of time.](#)  
[§ 160.528 Motions.](#)  
[§ 160.530 Sanctions.](#)  
[§ 160.532 Collateral estoppel.](#)  
[§ 160.534 The hearing.](#)  
[§ 160.536 Statistical sampling.](#)  
[§ 160.538 Witnesses.](#)  
[§ 160.540 Evidence.](#)  
[§ 160.542 The record.](#)  
[§ 160.544 Post hearing briefs.](#)  
[§ 160.546 ALJ's decision.](#)  
[§ 160.548 Appeal of the ALJ's decision.](#)  
[§ 160.550 Stay of the Secretary's decision.](#)  
[§ 160.552 Harmless error.](#)

---

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); 5 U.S.C. 552; secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279; and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.

SOURCE: 65 FR 82798, Dec. 28, 2000, unless otherwise noted.

#### **Subpart A—General Provisions**

##### **§ 160.101 Statutory basis and purpose.**

The requirements of this subchapter implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

[78 FR 5687, Jan. 25, 2013]

**§ 160.102 Applicability.**

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

**§ 160.103 Definitions.**

Except as otherwise provided, the following definitions apply to this subchapter:

*Act* means the Social Security Act.

*Administrative simplification provision* means any

requirement or prohibition established by:

- (1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;
- (2) Section 264 of Pub. L. 104-191;
- (3) Sections 13400-13424 of Public Law 111-5; or
- (4) This subchapter.

*ALJ* means Administrative Law Judge.

*ANSI* stands for the American National Standards Institute.

*Business associate:* (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in

§ 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance

issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

*Civil money penalty or penalty* means the amount determined under § 160.404 of this part and includes the plural of these terms.

*CMS* stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

*Compliance date* means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

*Covered entity* means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

*Disclosure* means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

*EIN* stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

- (1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.
- (2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

*Electronic media* means:

- (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as

magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

*Electronic protected health information* means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of *protected health information* as specified in this section.

*Employer* is defined as it is in 26 U.S.C. 3401(d).

*Family member* means, with respect to an individual:

- (1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
- (2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one

parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

*Genetic information* means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

*Genetic services* means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

*Genetic test* means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

*Group health plan* (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance,

reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

*HHS* stands for the Department of Health and Human Services.

*Health care* means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

*Health care clearinghouse* means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data

elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

*Health care provider* means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

*Health information* means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

*Health insurance issuer* (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the

business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

*Health maintenance organization (HMO)* (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

*Health plan* means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

*Implementation specification* means specific requirements or instructions for implementing a standard.

*Individual* means the person who is the subject of protected health information.

*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan,

employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

*Manifestation or manifested* means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

*Modify or modification* refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification.

*Organized health care arrangement* means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than

one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

*Person* means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

*Protected health information* means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

*Respondent* means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

*Secretary* means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

*Small health plan* means a health plan with annual receipts of \$5 million or less.

*Standard* means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

*Standard setting organization* (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

*State* refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

*Subcontractor* means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

*Trading partner agreement* means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

*Transaction* means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

*Use* means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

*Violation* or *violate* means, as the context may require, failure to comply with an administrative simplification provision.

*Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or

not they are paid by the covered entity or business associate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002; 67 FR 53266, Aug. 14, 2002; 68 FR 8374, Feb. 20, 2003; 71 FR 8424, Feb. 16, 2006; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 78 FR 5687, Jan. 25, 2013]

#### **§ 160.104 Modifications.**

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002]

#### **§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.**

Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.

[78 FR 5689, Jan. 25, 2013]

#### **Subpart B—Preemption of State Law**

##### **§ 160.201 Statutory basis.**

The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.

[78 FR 5689, Jan. 25, 2013]



**§ 160.202 Definitions.**

For purposes of this subpart, the following terms have the following meanings:

*Contrary*, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

*More stringent* means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

*Relates to the privacy of individually identifiable health information* means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

*State law* means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 74 FR 42767, Aug. 24, 2009; 78 FR 5689, Jan. 25, 2013]

**§ 160.203 General rule and exceptions.**

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]

#### **§ 160.204 Process for requesting exception determinations.**

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the FEDERAL REGISTER. Until the Secretary's determination is made, the standard, requirement,

or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

#### **§ 160.205 Duration of effectiveness of exception determinations.**

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

#### **Subpart C—Compliance and Investigations**

SOURCE: 71 FR 8424, Feb. 16, 2006, unless otherwise noted.

#### **§ 160.300 Applicability.**

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

[78 FR 5690, Jan. 25, 2013]

**§ 160.302 [Reserved]**

**§ 160.304 Principles for achieving compliance.**

(a) *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

[78 FR 5690, Jan. 25, 2013]

**§ 160.306 Complaints to the Secretary.**

(a) *Right to file a complaint.* A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

(b) *Requirements for filing complaints.* Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the FEDERAL REGISTER.

(c) *Investigation.* (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

[71 FR 8424, Feb. 16, 2006, as amended at 78 FR 5690, Jan. 25, 2013]

**§ 160.308 Compliance reviews.**

(a) The Secretary will conduct a compliance review to determine

whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

[78 FR 5690, Jan. 25, 2013]

**§ 160.310 Responsibilities of covered entities and business associates.**

(a) *Provide records and compliance reports.* A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

*(c) Permit access to information.*

(1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

[78 FR 5690, Jan. 25, 2013]

**§ 160.312 Secretarial action regarding complaints and compliance reviews.**

*(a) Resolution when noncompliance is indicated.* (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of

such finding in a notice of proposed determination in accordance with § 160.420 of this part.

*(b) Resolution when no violation is found.* If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

[78 FR 5690, Jan. 25, 2013]

**§ 160.314 Investigational subpoenas and inquiries.**

(a) The Secretary may issue subpoenas in accordance with 42 U.S.C. 405(d) and (e), 1320a-7a(j), and 1320d-5 to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review pursuant to this part. For purposes of this paragraph, a person other than a natural person is termed an “entity.”

(1) A subpoena issued under this paragraph must—

(i) State the name of the person (including the entity, if applicable) to whom the subpoena is addressed;

(ii) State the statutory authority for the subpoena;

(iii) Indicate the date, time, and place that the testimony will take place;

(iv) Include a reasonably specific description of any

documents or items required to be produced; and

(v) If the subpoena is addressed to an entity, describe with reasonable particularity the subject matter on which testimony is required. In that event, the entity must designate one or more natural persons who will testify on its behalf, and must state as to each such person that person's name and address and the matters on which he or she will testify. The designated person must testify as to matters known or reasonably available to the entity.

(2) A subpoena under this section must be served by—

(i) Delivering a copy to the natural person named in the subpoena or to the entity named in the subpoena at its last principal place of business; or

(ii) Registered or certified mail addressed to the natural person at his or her last known dwelling place or to the entity at its last known principal place of business.

(3) A verified return by the natural person serving the subpoena setting forth the manner of service or, in the case of service by registered or certified mail, the signed return post office receipt, constitutes proof of service.

(4) Witnesses are entitled to the same fees and mileage as witnesses in the district courts of the United States (28 U.S.C. 1821 and 1825). Fees need not be paid at the time the subpoena is served.

(5) A subpoena under this section is enforceable through the district court of the United States for the district where the subpoenaed natural person resides or is found or where the entity transacts business.

(b) Investigational inquiries are non-public investigational proceedings conducted by the Secretary.

(1) Testimony at investigational inquiries will be taken under oath or affirmation.

(2) Attendance of non-witnesses is discretionary with the Secretary, except that a witness is entitled to be accompanied, represented, and advised by an attorney.

(3) Representatives of the Secretary are entitled to attend and ask questions.

(4) A witness will have the opportunity to clarify his or her answers on the record following questioning by the Secretary.

(5) Any claim of privilege must be asserted by the witness on the record.

(6) Objections must be asserted on the record. Errors of any kind that might be corrected if promptly presented will be deemed to be waived unless reasonable objection is made at the investigational inquiry. Except where the objection is on the grounds of privilege, the question will be answered on the record, subject to objection.

(7) If a witness refuses to answer any question not privileged or to produce requested documents or items, or engages in conduct likely to

delay or obstruct the investigational inquiry, the Secretary may seek enforcement of the subpoena under paragraph (a)(5) of this section.

(8) The proceedings will be recorded and transcribed. The witness is entitled to a copy of the transcript, upon payment of prescribed costs, except that, for good cause, the witness may be limited to inspection of the official transcript of his or her testimony.

(9)(i) The transcript will be submitted to the witness for signature.

(A) Where the witness will be provided a copy of the transcript, the transcript will be submitted to the witness for signature. The witness may submit to the Secretary written proposed corrections to the transcript, with such corrections attached to the transcript. If the witness does not return a signed copy of the transcript or proposed corrections within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of its being submitted to him or her for signature, the witness will be deemed to have agreed that the transcript is true and accurate.

(B) Where, as provided in paragraph (b)(8) of this section, the witness is limited to inspecting the transcript, the witness will have the opportunity at the time of inspection to propose corrections to the transcript, with corrections attached to the transcript. The witness will also have the opportunity to sign the transcript. If the witness does not sign the transcript or offer corrections within 30 days (computed in the same manner

as prescribed under § 160.526 of this part) of receipt of notice of the opportunity to inspect the transcript, the witness will be deemed to have agreed that the transcript is true and accurate.

(ii) The Secretary's proposed corrections to the record of transcript will be attached to the transcript.

(c) Consistent with § 160.310(c)(3), testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in any administrative or judicial proceeding.

**§ 160.316 Refraining from intimidation or retaliation.**

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

(a) Filing of a complaint under § 160.306;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part; or

(c) Opposing any act or practice made unlawful by this subchapter, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of subpart E of part 164 of this subchapter.

[71 FR 8426, Feb. 16, 2006, as amended at 78 FR 5691, Jan. 25, 2013]

**Subpart D—Imposition of Civil Money Penalties**

SOURCE: 71 FR 8426, Feb. 16, 2006, unless otherwise noted.

**§ 160.400 Applicability.**

This subpart applies to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

**§ 160.401 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

*Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

*Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[74 FR 56130, Oct. 30, 2009, as amended at 78 FR 5691, Jan. 25, 2013]

**§ 160.402 Basis for a civil money penalty.**

(a) *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) *Violation by more than one covered entity or business associate.* (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) *Violation attributed to a covered entity or business associate.* (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

[78 FR 5691, Jan. 25, 2013]

**§ 160.404 Amount of a civil money penalty.**

(a) The amount of a civil money penalty will be determined in accordance with paragraph (b) of this section and §§ 160.406, 160.408, and 160.412.

(b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

(1) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty—

(i) In the amount of more than \$100 for each violation; or

(ii) In excess of \$25,000 for identical violations during a calendar year (January 1 through the following December 31);

(2) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty—

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

(A) In the amount of less than \$100 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,

(A) In the amount of less than \$1,000 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than \$10,000 or more than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would

have known that the violation occurred,

(A) In the amount of less than \$50,000 for each violation; or

(B) In excess of \$1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

(3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56130, Oct. 30, 2009; 78 FR 5691, Jan. 25, 2013]

**§ 160.406 Violations of an identical requirement or prohibition.**

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

[78 FR 5691, Jan. 25, 2013]

**§ 160.408 Factors considered in determining the amount of a civil money penalty.**

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar

to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

[78 FR 5691, Jan. 25, 2013]

**§ 160.410 Affirmative defenses.**

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on

a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d-6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:



(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

[78 FR 5692, Jan. 25, 2013]

**§ 160.412 Waiver.**

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the

payment of the penalty would be excessive relative to the violation.

[8 FR 5692, Jan. 25, 2013]

**§ 160.414 Limitations.**

No action under this subpart may be entertained unless commenced by the Secretary, in accordance with § 160.420, within 6 years from the date of the occurrence of the violation.

**§ 160.416 Authority to settle.**

Nothing in this subpart limits the authority of the Secretary to settle any issue or case or to compromise any penalty.

**§ 160.418 Penalty not exclusive.**

Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1) and 42 U.S.C. 299b-22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

[78 FR 5692, Jan. 25, 2013]

**§ 160.420 Notice of proposed determination.**

(a) If a penalty is proposed in accordance with this part, the Secretary must deliver, or send by certified mail with return receipt requested, to the respondent, written notice of the Secretary's intent to impose a penalty. This notice of proposed determination must include—

(1) Reference to the statutory basis for the penalty;

(2) A description of the findings of fact regarding the violations with respect to which the

penalty is proposed (except that, in any case where the Secretary is relying upon a statistical sampling study in accordance with § 160.536 of this part, the notice must provide a copy of the study relied upon by the Secretary);

(3) The reason(s) why the violation(s) subject(s) the respondent to a penalty;

(4) The amount of the proposed penalty and a reference to the subparagraph of § 160.404 upon which it is based.

(5) Any circumstances described in § 160.408 that were considered in determining the amount of the proposed penalty; and

(6) Instructions for responding to the notice, including a statement of the respondent's right to a hearing, a statement that failure to request a hearing within 90 days permits the imposition of the proposed penalty without the right to a hearing under § 160.504 or a right of appeal under § 160.548 of this part, and the address to which the hearing request must be sent.

(b) The respondent may request a hearing before an ALJ on the proposed penalty by filing a request in accordance with § 160.504 of this part.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56131, Oct. 30, 2009]

**§ 160.422 Failure to request a hearing.**

If the respondent does not request a hearing within the time prescribed by § 160.504 of this

part and the matter is not settled pursuant to § 160.416, the Secretary will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5. The Secretary will notify the respondent by certified mail, return receipt requested, of any penalty that has been imposed and of the means by which the respondent may satisfy the penalty, and the penalty is final on receipt of the notice. The respondent has no right to appeal a penalty under § 160.548 of this part with respect to which the respondent has not timely requested a hearing.

**§ 160.424 Collection of penalty.**

(a) Once a determination of the Secretary to impose a penalty has become final, the penalty will be collected by the Secretary, subject to the first sentence of 42 U.S.C. 1320a-7a(f).

(b) The penalty may be recovered in a civil action brought in the United States district court for the district where the respondent resides, is found, or is located.

(c) The amount of a penalty, when finally determined, or the amount agreed upon in compromise, may be deducted from any sum then or later owing by the United States, or by a State agency, to the respondent.

(d) Matters that were raised or that could have been raised in a hearing before an ALJ, or in an appeal under 42 U.S.C. 1320a-7a(e), may not be raised as a defense in a civil action by the United States to collect a penalty under this part.

**§ 160.426 Notification of the public and other agencies.**

Whenever a proposed penalty becomes final, the Secretary will notify, in such manner as the Secretary deems appropriate, the public and the following organizations and entities thereof and the reason it was imposed: the appropriate State or local medical or professional organization, the appropriate State agency or agencies administering or supervising the administration of State health care programs (as defined in 42 U.S.C. 1320a-7(h)), the appropriate utilization and quality control peer review organization, and the appropriate State or local licensing agency or organization (including the agency specified in 42 U.S.C. 1395aa(a), 1396a(a)(33)).

**Subpart E—Procedures for Hearings**

SOURCE: 71 FR 8428, Feb. 16, 2006, unless otherwise noted.

**§ 160.500 Applicability.**

This subpart applies to hearings conducted relating to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

**§ 160.502 Definitions.**

As used in this subpart, the following term has the following meaning:

*Board* means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three.

**§ 160.504 Hearing before an ALJ.**

(a) A respondent may request a hearing before an ALJ. The parties to the hearing proceeding consist of—

(1) The respondent; and

(2) The officer(s) or employee(s) of HHS to whom the enforcement authority involved has been delegated.

(b) The request for a hearing must be made in writing signed by the respondent or by the respondent's attorney and sent by certified mail, return receipt requested, to the address specified in the notice of proposed determination. The request for a hearing must be mailed within 90 days after notice of the proposed determination is received by the respondent. For purposes of this section, the respondent's date of receipt of the notice of proposed determination is presumed to be 5 days after the date of the notice unless the respondent makes a reasonable showing to the contrary to the ALJ.

(c) The request for a hearing must clearly and directly admit, deny, or explain each of the findings of fact contained in the notice of proposed determination with regard to which the respondent has any knowledge. If the respondent has no knowledge of a particular finding of fact and so states, the finding shall be deemed denied. The request for a hearing must also state the circumstances or arguments that the respondent alleges constitute the grounds for any defense and the factual and legal basis for opposing the penalty, except that a respondent may raise an affirmative defense

under § 160.410(b)(1) at any time.

(d) The ALJ must dismiss a hearing request where—

(1) On motion of the Secretary, the ALJ determines that the respondent's hearing request is not timely filed as required by paragraphs (b) or does not meet the requirements of paragraph (c) of this section;

(2) The respondent withdraws the request for a hearing;

(3) The respondent abandons the request for a hearing; or

(4) The respondent's hearing request fails to raise any issue that may properly be addressed in a hearing.

**§ 160.506 Rights of the parties.**

(a) Except as otherwise limited by this subpart, each party may—

(1) Be accompanied, represented, and advised by an attorney;

(2) Participate in any conference held by the ALJ;

(3) Conduct discovery of documents as permitted by this subpart;

(4) Agree to stipulations of fact or law that will be made part of the record;

(5) Present evidence relevant to the issues at the hearing;

(6) Present and cross-examine witnesses;

(7) Present oral arguments at the hearing as permitted by the ALJ; and

(8) Submit written briefs and proposed findings of fact and conclusions of law after the hearing.

(b) A party may appear in person or by a representative. Natural persons who appear as an attorney or other representative must conform to the standards of conduct and ethics required of practitioners before the courts of the United States.

(c) Fees for any services performed on behalf of a party by an attorney are not subject to the provisions of 42 U.S.C. 406, which authorizes the Secretary to specify or limit their fees.

**§ 160.508 Authority of the ALJ.**

(a) The ALJ must conduct a fair and impartial hearing, avoid delay, maintain order, and ensure that a record of the proceeding is made.

(b) The ALJ may—

(1) Set and change the date, time and place of the hearing upon reasonable notice to the parties;

(2) Continue or recess the hearing in whole or in part for a reasonable period of time;

(3) Hold conferences to identify or simplify the issues, or to consider other matters that may aid in the expeditious disposition of the proceeding;

(4) Administer oaths and affirmations;

(5) Issue subpoenas requiring the attendance of witnesses at hearings and the production of documents at or in relation to hearings;

(6) Rule on motions and other procedural matters;

(7) Regulate the scope and timing of documentary discovery as permitted by this subpart;

(8) Regulate the course of the hearing and the conduct of representatives, parties, and witnesses;

(9) Examine witnesses;

(10) Receive, rule on, exclude, or limit evidence;

(11) Upon motion of a party, take official notice of facts;

(12) Conduct any conference, argument or hearing in person or, upon agreement of the parties, by telephone; and

(13) Upon motion of a party, decide cases, in whole or in part, by summary judgment where there is no disputed issue of material fact. A summary judgment decision constitutes a hearing on the record for the purposes of this subpart.

(c) The ALJ—

(1) May not find invalid or refuse to follow Federal statutes, regulations, or Secretarial delegations of authority and must give deference to published guidance to the extent not inconsistent with statute or regulation;

(2) May not enter an order in the nature of a directed verdict;

(3) May not compel settlement negotiations;

(4) May not enjoin any act of the Secretary; or

(5) May not review the exercise of discretion by the Secretary with respect to whether to grant an extension under § 160.410(b)(2)(ii)(B) or (c)(2)(ii) of this part or to provide technical assistance under 42 U.S.C. 1320d-5(b)(2)(B).

**§ 160.510 Ex parte contacts.**

No party or person (except employees of the ALJ's office) may communicate in any way with the ALJ on any matter at issue in a case, unless on notice and opportunity for both parties to participate. This provision does not prohibit a party or person from inquiring about the status of a case or asking routine questions concerning administrative functions or procedures.

**§ 160.512 Prehearing conferences.**

(a) The ALJ must schedule at least one prehearing conference, and may schedule additional prehearing conferences as appropriate, upon reasonable notice, which may not be less than 14 business days, to the parties.

(b) The ALJ may use prehearing conferences to discuss the following—

(1) Simplification of the issues;

(2) The necessity or desirability of amendments to the pleadings, including the need for a more definite statement;

(3) Stipulations and admissions of fact or as to the contents and authenticity of documents;

(4) Whether the parties can agree to submission of the case on a stipulated record;

(5) Whether a party chooses to waive appearance at an oral hearing and to submit only documentary evidence (subject to the objection of the other party) and written argument;

(6) Limitation of the number of witnesses;

(7) Scheduling dates for the exchange of witness lists and of proposed exhibits;

(8) Discovery of documents as permitted by this subpart;

(9) The time and place for the hearing;

(10) The potential for the settlement of the case by the parties; and

(11) Other matters as may tend to encourage the fair, just and expeditious disposition of the proceedings, including the protection of privacy of individually identifiable health information that may be submitted into evidence or otherwise used in the proceeding, if appropriate.

(c) The ALJ must issue an order containing the matters agreed upon by the parties or ordered by the ALJ at a prehearing conference.

**§ 160.514 Authority to settle.**

The Secretary has exclusive authority to settle any issue or case without the consent of the ALJ.

**§ 160.516 Discovery.**

(a) A party may make a request to another party for production of documents for inspection and copying that are relevant and material to the issues before the ALJ.

(b) For the purpose of this section, the term “documents” includes information, reports, answers, records, accounts, papers and other data and documentary evidence. Nothing contained in this section may be interpreted to require the creation of a document, except that requested data stored in an electronic data storage system must be produced in a form accessible to the requesting party.

(c) Requests for documents, requests for admissions, written interrogatories, depositions and any forms of discovery, other than those permitted under paragraph (a) of this section, are not authorized.

(d) This section may not be construed to require the disclosure of interview reports or statements obtained by any party, or on behalf of any party, of persons who will not be called as witnesses by that party, or analyses and summaries prepared in conjunction with the investigation or litigation of the case, or any otherwise privileged documents.

(e)(1) When a request for production of documents has

been received, within 30 days the party receiving that request must either fully respond to the request, or state that the request is being objected to and the reasons for that objection. If objection is made to part of an item or category, the part must be specified. Upon receiving any objections, the party seeking production may then, within 30 days or any other time frame set by the ALJ, file a motion for an order compelling discovery. The party receiving a request for production may also file a motion for protective order any time before the date the production is due.

(2) The ALJ may grant a motion for protective order or deny a motion for an order compelling discovery if the ALJ finds that the discovery sought—

(i) Is irrelevant;

(ii) Is unduly costly or burdensome;

(iii) Will unduly delay the proceeding; or

(iv) Seeks privileged information.

(3) The ALJ may extend any of the time frames set forth in paragraph (e)(1) of this section.

(4) The burden of showing that discovery should be allowed is on the party seeking discovery.

**§ 160.518 Exchange of witness lists, witness statements, and exhibits.**

(a) The parties must exchange witness lists, copies of prior written statements of proposed witnesses, and copies of proposed hearing exhibits,

including copies of any written statements that the party intends to offer in lieu of live testimony in accordance with § 160.538, not more than 60, and not less than 15, days before the scheduled hearing, except that if a respondent intends to introduce the evidence of a statistical expert, the respondent must provide the Secretarial party with a copy of the statistical expert's report not less than 30 days before the scheduled hearing.

(b)(1) If, at any time, a party objects to the proposed admission of evidence not exchanged in accordance with paragraph (a) of this section, the ALJ must determine whether the failure to comply with paragraph (a) of this section should result in the exclusion of that evidence.

(2) Unless the ALJ finds that extraordinary circumstances justified the failure timely to exchange the information listed under paragraph (a) of this section, the ALJ must exclude from the party's case-in-chief—

(i) The testimony of any witness whose name does not appear on the witness list; and

(ii) Any exhibit not provided to the opposing party as specified in paragraph (a) of this section.

(3) If the ALJ finds that extraordinary circumstances existed, the ALJ must then determine whether the admission of that evidence would cause substantial prejudice to the objecting party.

(i) If the ALJ finds that there is no substantial prejudice, the evidence may be admitted.

(ii) If the ALJ finds that there is substantial prejudice, the ALJ may exclude the evidence, or, if he or she does not exclude the evidence, must postpone the hearing for such time as is necessary for the objecting party to prepare and respond to the evidence, unless the objecting party waives postponement.

(c) Unless the other party objects within a reasonable period of time before the hearing, documents exchanged in accordance with paragraph (a) of this section will be deemed to be authentic for the purpose of admissibility at the hearing.

**§ 160.520 Subpoenas for attendance at hearing.**

(a) A party wishing to procure the appearance and testimony of any person at the hearing may make a motion requesting the ALJ to issue a subpoena if the appearance and testimony are reasonably necessary for the presentation of a party's case.

(b) A subpoena requiring the attendance of a person in accordance with paragraph (a) of this section may also require the person (whether or not the person is a party) to produce relevant and material evidence at or before the hearing.

(c) When a subpoena is served by a respondent on a particular employee or official or particular office of HHS, the Secretary may comply by designating any knowledgeable HHS representative to appear and testify.

(d) A party seeking a subpoena must file a written motion not less than 30 days before the date fixed for the hearing, unless otherwise allowed by the ALJ

for good cause shown. That motion must—

- (1) Specify any evidence to be produced;
- (2) Designate the witnesses; and
- (3) Describe the address and location with sufficient particularity to permit those witnesses to be found.
- (e) The subpoena must specify the time and place at which the witness is to appear and any evidence the witness is to produce.
- (f) Within 15 days after the written motion requesting issuance of a subpoena is served, any party may file an opposition or other response.
- (g) If the motion requesting issuance of a subpoena is granted, the party seeking the subpoena must serve it by delivery to the person named, or by certified mail addressed to that person at the person's last dwelling place or principal place of business.
- (h) The person to whom the subpoena is directed may file with the ALJ a motion to quash the subpoena within 10 days after service.
- (i) The exclusive remedy for contumacy by, or refusal to obey a subpoena duly served upon, any person is specified in 42 U.S.C. 405(e).

**§ 160.522 Fees.**

The party requesting a subpoena must pay the cost of the fees and mileage of any witness subpoenaed in the amounts that would be payable to a witness in

a proceeding in United States District Court. A check for witness fees and mileage must accompany the subpoena when served, except that, when a subpoena is issued on behalf of the Secretary, a check for witness fees and mileage need not accompany the subpoena.

**§ 160.524 Form, filing, and service of papers.**

- (a) *Forms.* (1) Unless the ALJ directs the parties to do otherwise, documents filed with the ALJ must include an original and two copies.
- (2) Every pleading and paper filed in the proceeding must contain a caption setting forth the title of the action, the case number, and a designation of the paper, such as motion to quash subpoena.
- (3) Every pleading and paper must be signed by and must contain the address and telephone number of the party or the person on whose behalf the paper was filed, or his or her representative.
- (4) Papers are considered filed when they are mailed.
- (b) *Service.* A party filing a document with the ALJ or the Board must, at the time of filing, serve a copy of the document on the other party. Service upon any party of any document must be made by delivering a copy, or placing a copy of the document in the United States mail, postage prepaid and addressed, or with a private delivery service, to the party's last known address. When a party is represented by an attorney, service must be made upon the attorney in lieu of the party.

(c) *Proof of service.* A certificate of the natural person serving the document by personal delivery or by mail, setting forth the manner of service, constitutes proof of service.

**§ 160.526 Computation of time.**

- (a) In computing any period of time under this subpart or in an order issued thereunder, the time begins with the day following the act, event or default, and includes the last day of the period unless it is a Saturday, Sunday, or legal holiday observed by the Federal Government, in which event it includes the next business day.
- (b) When the period of time allowed is less than 7 days, intermediate Saturdays, Sundays, and legal holidays observed by the Federal Government must be excluded from the computation.
- (c) Where a document has been served or issued by placing it in the mail, an additional 5 days must be added to the time permitted for any response. This paragraph does not apply to requests for hearing under § 160.504.

**§ 160.528 Motions.**

- (a) An application to the ALJ for an order or ruling must be by motion. Motions must state the relief sought, the authority relied upon and the facts alleged, and must be filed with the ALJ and served on all other parties.
- (b) Except for motions made during a prehearing conference or at the hearing, all motions must be in writing. The ALJ

may require that oral motions be reduced to writing.

(c) Within 10 days after a written motion is served, or such other time as may be fixed by the ALJ, any party may file a response to the motion.

(d) The ALJ may not grant a written motion before the time for filing responses has expired, except upon consent of the parties or following a hearing on the motion, but may overrule or deny the motion without awaiting a response.

(e) The ALJ must make a reasonable effort to dispose of all outstanding motions before the beginning of the hearing.

#### **§ 160.530 Sanctions.**

The ALJ may sanction a person, including any party or attorney, for failing to comply with an order or procedure, for failing to defend an action or for other misconduct that interferes with the speedy, orderly or fair conduct of the hearing. The sanctions must reasonably relate to the severity and nature of the failure or misconduct. The sanctions may include—

(a) In the case of refusal to provide or permit discovery under the terms of this part, drawing negative factual inferences or treating the refusal as an admission by deeming the matter, or certain facts, to be established;

(b) Prohibiting a party from introducing certain evidence or otherwise supporting a particular claim or defense;

(c) Striking pleadings, in whole or in part;

(d) Staying the proceedings;

(e) Dismissal of the action;

(f) Entering a decision by default;

(g) Ordering the party or attorney to pay the attorney's fees and other costs caused by the failure or misconduct; and

(h) Refusing to consider any motion or other action that is not filed in a timely manner.

#### **§ 160.532 Collateral estoppel.**

When a final determination that the respondent violated an administrative simplification provision has been rendered in any proceeding in which the respondent was a party and had an opportunity to be heard, the respondent is bound by that determination in any proceeding under this part.

#### **§ 160.534 The hearing.**

(a) The ALJ must conduct a hearing on the record in order to determine whether the respondent should be found liable under this part.

(b) (1) The respondent has the burden of going forward and the burden of persuasion with respect to any:

(i) Affirmative defense pursuant to § 160.410 of this part;

(ii) Challenge to the amount of a proposed penalty pursuant to §§ 160.404-160.408 of this part, including any factors raised as mitigating factors; or

(iii) Claim that a proposed penalty should be reduced or

waived pursuant to § 160.412 of this part; and

(iv) Compliance with subpart D of part 164, as provided under § 164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

(3) The burden of persuasion will be judged by a preponderance of the evidence.

(c) The hearing must be open to the public unless otherwise ordered by the ALJ for good cause shown.

(d)(1) Subject to the 15-day rule under § 160.518(a) and the admissibility of evidence under § 160.540, either party may introduce, during its case in chief, items or information that arose or became known after the date of the issuance of the notice of proposed determination or the request for hearing, as applicable. Such items and information may not be admitted into evidence, if introduced—

(i) By the Secretary, unless they are material and relevant to the acts or omissions with respect to which the penalty is proposed in the notice of proposed determination pursuant to § 160.420 of this part, including circumstances that may increase penalties; or

(ii) By the respondent, unless they are material and relevant to an admission, denial or

explanation of a finding of fact in the notice of proposed determination under § 160.420 of this part, or to a specific circumstance or argument expressly stated in the request for hearing under § 160.504, including circumstances that may reduce penalties.

(2) After both parties have presented their cases, evidence may be admitted in rebuttal even if not previously exchanged in accordance with § 160.518.

[71 FR 8428, Feb. 16, 2006, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5692, Jan. 25, 2013]

**§ 160.536 Statistical sampling.**

(a) In meeting the burden of proof set forth in § 160.534, the Secretary may introduce the results of a statistical sampling study as evidence of the number of violations under § 160.406 of this part, or the factors considered in determining the amount of the civil money penalty under § 160.408 of this part. Such statistical sampling study, if based upon an appropriate sampling and computed by valid statistical methods, constitutes prima facie evidence of the number of violations and the existence of factors material to the proposed civil money penalty as described in §§ 160.406 and 160.408.

(b) Once the Secretary has made a prima facie case, as described in paragraph (a) of this section, the burden of going forward shifts to the respondent to produce evidence reasonably calculated to rebut the findings of the statistical sampling study. The Secretary will then be given

the opportunity to rebut this evidence.

**§ 160.538 Witnesses.**

(a) Except as provided in paragraph (b) of this section, testimony at the hearing must be given orally by witnesses under oath or affirmation.

(b) At the discretion of the ALJ, testimony of witnesses other than the testimony of expert witnesses may be admitted in the form of a written statement. The ALJ may, at his or her discretion, admit prior sworn testimony of experts that has been subject to adverse examination, such as a deposition or trial testimony. Any such written statement must be provided to the other party, along with the last known address of the witness, in a manner that allows sufficient time for the other party to subpoena the witness for cross-examination at the hearing. Prior written statements of witnesses proposed to testify at the hearing must be exchanged as provided in § 160.518.

(c) The ALJ must exercise reasonable control over the mode and order of interrogating witnesses and presenting evidence so as to:

(1) Make the interrogation and presentation effective for the ascertainment of the truth;

(2) Avoid repetition or needless consumption of time; and

(3) Protect witnesses from harassment or undue embarrassment.

(d) The ALJ must permit the parties to conduct cross-

examination of witnesses as may be required for a full and true disclosure of the facts.

(e) The ALJ may order witnesses excluded so that they cannot hear the testimony of other witnesses, except that the ALJ may not order to be excluded—

(1) A party who is a natural person;

(2) In the case of a party that is not a natural person, the officer or employee of the party appearing for the entity pro se or designated as the party's representative; or

(3) A natural person whose presence is shown by a party to be essential to the presentation of its case, including a person engaged in assisting the attorney for the Secretary.

**§ 160.540 Evidence.**

(a) The ALJ must determine the admissibility of evidence.

(b) Except as provided in this subpart, the ALJ is not bound by the Federal Rules of Evidence. However, the ALJ may apply the Federal Rules of Evidence where appropriate, for example, to exclude unreliable evidence.

(c) The ALJ must exclude irrelevant or immaterial evidence.

(d) Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or by considerations of undue delay or needless presentation of cumulative evidence.



(e) Although relevant, evidence must be excluded if it is privileged under Federal law.

(f) Evidence concerning offers of compromise or settlement are inadmissible to the extent provided in Rule 408 of the Federal Rules of Evidence.

(g) Evidence of crimes, wrongs, or acts other than those at issue in the instant case is admissible in order to show motive, opportunity, intent, knowledge, preparation, identity, lack of mistake, or existence of a scheme. This evidence is admissible regardless of whether the crimes, wrongs, or acts occurred during the statute of limitations period applicable to the acts or omissions that constitute the basis for liability in the case and regardless of whether they were referenced in the Secretary's notice of proposed determination under § 160.420 of this part.

(h) The ALJ must permit the parties to introduce rebuttal witnesses and evidence.

(i) All documents and other evidence offered or taken for the record must be open to examination by both parties, unless otherwise ordered by the ALJ for good cause shown.

**§ 160.542 The record.**

(a) The hearing must be recorded and transcribed. Transcripts may be obtained following the hearing from the ALJ. A party that requests a transcript of hearing proceedings must pay the cost of preparing the transcript unless, for good cause shown by the party, the payment is waived by the ALJ or the Board, as appropriate.

(b) The transcript of the testimony, exhibits, and other evidence admitted at the hearing, and all papers and requests filed in the proceeding constitute the record for decision by the ALJ and the Secretary.

(c) The record may be inspected and copied (upon payment of a reasonable fee) by any person, unless otherwise ordered by the ALJ for good cause shown.

(d) For good cause, the ALJ may order appropriate redactions made to the record.

**§ 160.544 Post hearing briefs.**

The ALJ may require the parties to file post-hearing briefs. In any event, any party may file a post-hearing brief. The ALJ must fix the time for filing the briefs. The time for filing may not exceed 60 days from the date the parties receive the transcript of the hearing or, if applicable, the stipulated record. The briefs may be accompanied by proposed findings of fact and conclusions of law. The ALJ may permit the parties to file reply briefs.

**§ 160.546 ALJ's decision.**

(a) The ALJ must issue a decision, based only on the record, which must contain findings of fact and conclusions of law.

(b) The ALJ may affirm, increase, or reduce the penalties imposed by the Secretary.

(c) The ALJ must issue the decision to both parties within 60 days after the time for submission of post-hearing briefs and reply briefs, if permitted, has expired. If the

ALJ fails to meet the deadline contained in this paragraph, he or she must notify the parties of the reason for the delay and set a new deadline.

(d) Unless the decision of the ALJ is timely appealed as provided for in § 160.548, the decision of the ALJ will be final and binding on the parties 60 days from the date of service of the ALJ's decision.

**§ 160.548 Appeal of the ALJ's decision.**

(a) Any party may appeal the decision of the ALJ to the Board by filing a notice of appeal with the Board within 30 days of the date of service of the ALJ decision. The Board may extend the initial 30 day period for a period of time not to exceed 30 days if a party files with the Board a request for an extension within the initial 30 day period and shows good cause.

(b) If a party files a timely notice of appeal with the Board, the ALJ must forward the record of the proceeding to the Board.

(c) A notice of appeal must be accompanied by a written brief specifying exceptions to the initial decision and reasons supporting the exceptions. Any party may file a brief in opposition to the exceptions, which may raise any relevant issue not addressed in the exceptions, within 30 days of receiving the notice of appeal and the accompanying brief. The Board may permit the parties to file reply briefs.

(d) There is no right to appear personally before the Board or to appeal to the Board any interlocutory ruling by the ALJ.

(e) Except for an affirmative defense under § 160.410(a)(1) or (2) of this part, the Board may not consider any issue not raised in the parties' briefs, nor any issue in the briefs that could have been raised before the ALJ but was not.

(f) If any party demonstrates to the satisfaction of the Board that additional evidence not presented at such hearing is relevant and material and that there were reasonable grounds for the failure to adduce such evidence at the hearing, the Board may remand the matter to the ALJ for consideration of such additional evidence.

(g) The Board may decline to review the case, or may affirm, increase, reduce, reverse or remand any penalty determined by the ALJ.

(h) The standard of review on a disputed issue of fact is whether the initial decision of the ALJ is supported by substantial evidence on the whole record. The standard of review on a disputed issue of law is whether the decision is erroneous.

(i) Within 60 days after the time for submission of briefs and reply briefs, if permitted, has expired, the Board must serve on each party to the appeal a copy of the Board's decision and a statement describing the right of any respondent who is penalized to seek judicial review.

(j)(1) The Board's decision under paragraph (i) of this section, including a decision to decline review of the initial decision, becomes the final decision of the Secretary 60 days after the date of service of the Board's decision, except

with respect to a decision to remand to the ALJ or if reconsideration is requested under this paragraph.

(2) The Board will reconsider its decision only if it determines that the decision contains a clear error of fact or error of law. New evidence will not be a basis for reconsideration unless the party demonstrates that the evidence is newly discovered and was not previously available.

(3) A party may file a motion for reconsideration with the Board before the date the decision becomes final under paragraph (j)(1) of this section. A motion for reconsideration must be accompanied by a written brief specifying any alleged error of fact or law and, if the party is relying on additional evidence, explaining why the evidence was not previously available. Any party may file a brief in opposition within 15 days of receiving the motion for reconsideration and the accompanying brief unless this time limit is extended by the Board for good cause shown. Reply briefs are not permitted.

(4) The Board must rule on the motion for reconsideration not later than 30 days from the date the opposition brief is due. If the Board denies the motion, the decision issued under paragraph (i) of this section becomes the final decision of the Secretary on the date of service of the ruling. If the Board grants the motion, the Board will issue a reconsidered decision, after such procedures as the Board determines necessary to address the effect of any error. The Board's decision on reconsideration becomes the final decision of the Secretary

on the date of service of the decision, except with respect to a decision to remand to the ALJ.

(5) If service of a ruling or decision issued under this section is by mail, the date of service will be deemed to be 5 days from the date of mailing.

(k)(1) A respondent's petition for judicial review must be filed within 60 days of the date on which the decision of the Board becomes the final decision of the Secretary under paragraph (j) of this section.

(2) In compliance with 28 U.S.C. 2112(a), a copy of any petition for judicial review filed in any U.S. Court of Appeals challenging the final decision of the Secretary must be sent by certified mail, return receipt requested, to the General Counsel of HHS. The petition copy must be a copy showing that it has been time-stamped by the clerk of the court when the original was filed with the court.

(3) If the General Counsel of HHS received two or more petitions within 10 days after the final decision of the Secretary, the General Counsel will notify the U.S. Judicial Panel on Multidistrict Litigation of any petitions that were received within the 10 day period.

#### **§ 160.550 Stay of the Secretary's decision.**

(a) Pending judicial review, the respondent may file a request for stay of the effective date of any penalty with the ALJ. The request must be accompanied by a copy of the notice of appeal filed with the Federal court. The filing of the request automatically stays the effective date of the penalty until such

time as the ALJ rules upon the request.

(b) The ALJ may not grant a respondent's request for stay of any penalty unless the respondent posts a bond or provides other adequate security.

(c) The ALJ must rule upon a respondent's request for stay within 10 days of receipt.

**§ 160.552 Harmless error.**

No error in either the admission or the exclusion of evidence, and no error or defect in any ruling or order or in any act done or omitted by the ALJ or by any of the parties is ground for vacating, modifying or otherwise disturbing an otherwise appropriate ruling or order or act, unless refusal to take such action appears to the ALJ or the Board inconsistent with substantial justice. The ALJ and the Board at every stage of the proceeding must disregard any error or defect in the proceeding that does not affect the substantial rights of the parties.

---

**PART 162—  
ADMINISTRATIVE  
REQUIREMENTS**

---

**Contents**

Subpart A—General Provisions

§ 162.100 Applicability.  
§ 162.103 Definitions.

Subparts B-C [Reserved]

Subpart D—Standard Unique  
Health Identifier for Health Care  
Providers

§ 162.402 [Reserved]  
§ 162.404 Compliance dates of  
the implementation of the  
standard unique health identifier  
for health care providers.  
§ 162.406 Standard unique  
health identifier for health care  
providers.  
§ 162.408 National Provider  
System.  
§ 162.410 Implementation  
specifications: Health care  
providers.  
§ 162.412 Implementation  
specifications: Health plans.  
§ 162.414 Implementation  
specifications: Health care  
clearinghouses.

Subpart E—Standard Unique  
Health Identifier for Health  
Plans

§ 162.502 [Reserved]  
§ 162.504 Compliance  
requirements for the  
implementation of the standard  
unique health plan identifier.  
§ 162.506 Standard unique  
health plan identifier.  
§ 162.508 Enumeration  
System.  
§ 162.510 Full implementation  
requirements: Covered entities.

§ 162.512 Implementation  
specifications: Health plans.  
§ 162.514 Other entity  
identifier.

Subpart F—Standard Unique  
Employer Identifier

§ 162.600 Compliance dates of  
the implementation of the  
standard unique employer  
identifier.  
§ 162.605 Standard unique  
employer identifier.  
§ 162.610 Implementation  
specifications for covered  
entities.

Subparts G-H [Reserved]

Subpart I—General Provisions  
for Transactions

§ 162.900 [Reserved]  
§ 162.910 Maintenance of  
standards and adoption of  
modifications and new  
standards.  
§ 162.915 Trading partner  
agreements.  
§ 162.920 Availability of  
implementation specifications  
and operating rules.  
§ 162.923 Requirements for  
covered entities.  
§ 162.925 Additional  
requirements for health plans.  
§ 162.930 Additional rules for  
health care clearinghouses.  
§ 162.940 Exceptions from  
standards to permit testing of  
proposed modifications.

Subpart J—Code Sets

§ 162.1000 General  
requirements.  
§ 162.1002 Medical data code  
sets.  
§ 162.1011 Valid code sets.

Subpart K—Health Care Claims  
or Equivalent Encounter  
Information

§ 162.1101 Health care claims  
or equivalent encounter  
information transaction.  
§ 162.1102 Standards for  
health care claims or equivalent  
encounter information  
transaction.

Subpart L—Eligibility for a  
Health Plan

§ 162.1201 Eligibility for a  
health plan transaction.  
§ 162.1202 Standards for  
eligibility for a health plan  
transaction.  
§ 162.1203 Operating rules for  
eligibility for a health plan  
transaction.

Subpart M—Referral  
Certification and Authorization

§ 162.1301 Referral  
certification and authorization  
transaction.  
§ 162.1302 Standards for  
referral certification and  
authorization transaction.

Subpart N—Health Care Claim  
Status

§ 162.1401 Health care claim  
status transaction.  
§ 162.1402 Standards for  
health care claim status  
transaction.  
§ 162.1403 Operating rules for  
health care claim status  
transaction.

Subpart O—Enrollment and  
Disenrollment in a Health Plan

§ 162.1501 Enrollment and  
disenrollment in a health plan  
transaction.  
§ 162.1502 Standards for  
enrollment and disenrollment in  
a health plan transaction.

[Subpart P—Health Care  
Electronic Funds Transfers  
\(EFT\) and Remittance Advice](#)

[§ 162.1601 Health care  
electronic funds transfers \(EFT\)  
and remittance advice  
transaction.](#)

[§ 162.1602 Standards for  
health care electronic funds  
transfers \(EFT\) and remittance  
advice transaction.](#)

[§ 162.1603 Operating rules for  
health care electronic funds  
transfers \(EFT\) and remittance  
advice transaction.](#)

[Subpart Q—Health Plan  
Premium Payments](#)

[§ 162.1701 Health plan  
premium payments transaction.](#)

[§ 162.1702 Standards for  
health plan premium payments  
transaction.](#)

[Subpart R—Coordination of  
Benefits](#)

[§ 162.1801 Coordination of  
benefits transaction.](#)

[§ 162.1802 Standards for  
coordination of benefits  
information transaction.](#)

[Subpart S—Medicaid Pharmacy  
Subrogation](#)

[§ 162.1901 Medicaid  
pharmacy subrogation  
transaction.](#)

[§ 162.1902 Standard for  
Medicaid pharmacy subrogation  
transaction.](#)

---

AUTHORITY: Secs. 1171 through 1180 of the Social Security Act (42 U.S.C. 1320d-1320d-9), as added by sec. 262 of Pub. L. 104-191, 110 Stat. 2021-2031, sec. 105 of Pub. L. 110-233, 122 Stat. 881-922, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-

2034 (42 U.S.C. 1320d-2(note), and secs. 1104 and 10109 of Pub. L. 111-148, 124 Stat. 146-154 and 915-917.

SOURCE: 65 FR 50367, Aug. 17, 2000, unless otherwise noted.

**Subpart A—General  
Provisions**

**§ 162.100 Applicability.**

Covered entities (as defined in § 160.103 of this subchapter) must comply with the applicable requirements of this part.

**§ 162.103 Definitions.**

For purposes of this part, the following definitions apply:

*Code set* means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes.

*Code set maintaining organization* means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part.

*Controlling health plan (CHP)* means a health plan that—

(1) Controls its own business activities, actions, or policies; or

(2)(i) Is controlled by an entity that is not a health plan; and

(ii) If it has a subhealth plan(s) (as defined in this section), exercises sufficient control over the subhealth plan(s) to direct

its/their business activities, actions, or policies.

*Covered health care provider* means a health care provider that meets the definition at paragraph (3) of the definition of “covered entity” at § 160.103.

*Data condition* means the rule that describes the circumstances under which a covered entity must use a particular data element or segment.

*Data content* means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not data content.

*Data element* means the smallest named unit of information in a transaction.

*Data set* means a semantically meaningful unit of information exchanged between two parties to a transaction.

*Descriptor* means the text defining a code.

*Designated standard maintenance organization (DSMO)* means an organization designated by the Secretary under § 162.910(a).

*Direct data entry* means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer.

*Format* refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction.

*HCPCS* stands for the Health [Care Financing Administration] Common Procedure Coding System.

*Maintain* or *maintenance* refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification.

*Maximum defined data set* means all of the required data elements for a particular standard based on a specific implementation specification.

*Operating rules* means the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications as adopted for purposes of this part.

*Segment* means a group of related data elements in a transaction.

*Stage 1 payment initiation* means a health plan's order, instruction or authorization to its financial institution to make a health care claims payment using an electronic funds transfer (EFT) through the ACH Network.

*Standard transaction* means a transaction that complies with an applicable standard and associated operating rules adopted under this part.

*Subhealth plan (SHP)* means a health plan whose business activities, actions, or policies are directed by a controlling health plan.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8374, Feb. 20, 2003; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 77 FR 54719, Sept. 5, 2012]

#### **Subparts B-C [Reserved]**

#### **Subpart D—Standard Unique Health Identifier for Health Care Providers**

SOURCE: 69 FR 3468, Jan. 23, 2004, unless otherwise noted.

#### **§ 162.402 [Reserved]**

#### **§ 162.404 Compliance dates of the implementation of the standard unique health identifier for health care providers.**

(a) *Health care providers.* A covered health care provider must comply with the implementation specifications in § 162.410 no later than May 23, 2007.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.412 no later than one of the following dates:

(1) A health plan that is not a small health plan—May 23, 2007.

(2) A small health plan—May 23, 2008.

(c) *Health care clearinghouses.* A health care clearinghouse

must comply with the implementation specifications in § 162.414 no later than May 23, 2007.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

#### **§ 162.406 Standard unique health identifier for health care providers.**

(a) *Standard.* The standard unique health identifier for health care providers is the National Provider Identifier (NPI). The NPI is a 10-position numeric identifier, with a check digit in the 10th position, and no intelligence about the health care provider in the number.

(b) *Required and permitted uses for the NPI.* (1) The NPI must be used as stated in § 162.410, § 162.412, and § 162.414.

(2) The NPI may be used for any other lawful purpose.

#### **§ 162.408 National Provider System.**

*National Provider System.* The National Provider System (NPS) shall do the following:

(a) Assign a single, unique NPI to a health care provider, provided that—

(1) The NPS may assign an NPI to a subpart of a health care provider in accordance with paragraph (g); and

(2) The Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health

care provider that has been assigned an NPI and perform tasks necessary to update that information.

(c) If appropriate, deactivate an NPI upon receipt of appropriate information concerning the dissolution of the health care provider that is an organization, the death of the health care provider who is an individual, or other circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated NPI upon receipt of appropriate information.

(e) Not assign a deactivated NPI to any other health care provider.

(f) Disseminate NPS information upon approved requests.

(g) Assign an NPI to a subpart of a health care provider on request if the identifying data for the subpart are unique.

**§ 162.410 Implementation specifications: Health care providers.**

(a) A covered entity that is a covered health care provider must:

(1) Obtain, by application if necessary, an NPI from the National Provider System (NPS) for itself or for any subpart of the covered entity that would be a covered health care provider if it were a separate legal entity. A covered entity may obtain an NPI for any other subpart that qualifies for the assignment of an NPI.

(2) Use the NPI it obtained from the NPS to identify itself on all

standard transactions that it conducts where its health care provider identifier is required.

(3) Disclose its NPI, when requested, to any entity that needs the NPI to identify that covered health care provider in a standard transaction.

(4) Communicate to the NPS any changes in its required data elements in the NPS within 30 days of the change.

(5) If it uses one or more business associates to conduct standard transactions on its behalf, require its business associate(s) to use its NPI and other NPIs appropriately as required by the transactions that the business associate(s) conducts on its behalf.

(6) If it has been assigned NPIs for one or more subparts, comply with the requirements of paragraphs (a)(2) through (a)(5) of this section with respect to each of those NPIs.

(b) An organization covered health care provider that has as a member, employs, or contracts with, an individual health care provider who is not a covered entity and is a prescriber, must require such health care provider to—

(1) Obtain an NPI from the National Plan and Provider Enumeration System (NPPES); and

(2) To the extent the prescriber writes a prescription while acting within the scope of the prescriber's relationship with the organization, disclose the NPI upon request to any entity that needs it to identify the prescriber in a standard transaction.

(c) A health care provider that is not a covered entity may obtain, by application if necessary, an NPI from the NPS.

[69 FR 3468, Jan. 23, 2004, as amended at 77 FR 54719, Sept. 5, 2012]

**§ 162.412 Implementation specifications: Health plans.**

(a) A health plan must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

(b) A health plan may not require a health care provider that has been assigned an NPI to obtain an additional NPI.

**§ 162.414 Implementation specifications: Health care clearinghouses.**

A health care clearinghouse must use the NPI of any health care provider (or subpart(s), if applicable) that has been assigned an NPI to identify that health care provider on all standard transactions where that health care provider's identifier is required.

**Subpart E—Standard Unique Health Identifier for Health Plans**

SOURCE: 77 FR 54719, Sept. 5, 2012, unless otherwise noted.

**§ 162.502 [Reserved]**

**§ 162.504 Compliance requirements for the implementation of the standard unique health plan identifier.**

(a) *Covered entities.* A covered entity must comply with the implementation requirements in § 162.510 no later than November 7, 2016.

(b) *Health plans.* A health plan must comply with the implementation specifications in § 162.512 no later than one of the following dates:

(1) A health plan that is not a small health plan— November 5, 2014.

(2) A health plan that is a small health plan— November 5, 2015.

[77 FR 54719, Sept. 5, 2012, as amended at 77 FR 60630, Oct. 4, 2012]

**§ 162.506 Standard unique health plan identifier.**

(a) *Standard.* The standard unique health plan identifier is the Health Plan Identifier (HPID) that is assigned by the Enumeration System identified in § 162.508.

(b) *Required and permitted uses for the HPID.* (1) The HPID must be used as specified in § 162.510 and § 162.512.

(2) The HPID may be used for any other lawful purpose.

**§ 162.508 Enumeration System.**

The Enumeration System must do all of the following:

(a) Assign a single, unique—

(1) HPID to a health plan, provided that the Secretary has

sufficient information to permit the assignment to be made; or

(2) OEID to an entity eligible to receive one under § 162.514(a), provided that the Secretary has sufficient information to permit the assignment to be made.

(b) Collect and maintain information about each health plan that applies for or has been assigned an HPID and each entity that applies for or has been assigned an OEID, and perform tasks necessary to update that information.

(c) If appropriate, deactivate an HPID or OEID upon receipt of sufficient information concerning circumstances justifying deactivation.

(d) If appropriate, reactivate a deactivated HPID or OEID upon receipt of sufficient information justifying reactivation.

(e) Not assign a deactivated HPID to any other health plan or OEID to any other entity.

(f) Disseminate Enumeration System information upon approved requests.

**§ 162.510 Full implementation requirements: Covered entities.**

(a) A covered entity must use an HPID to identify a health plan that has an HPID when a covered entity identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

(b) If a covered entity uses one or more business associates to conduct standard transactions on its behalf, it must require its business associate(s) to use an

HPID to identify a health plan that has an HPID when the business associate(s) identifies a health plan in a transaction for which the Secretary has adopted a standard under this part.

**§ 162.512 Implementation specifications: Health plans.**

(a) A controlling health plan must do all of the following:

(1) Obtain an HPID from the Enumeration System for itself.

(2) Disclose its HPID, when requested, to any entity that needs the HPID to identify the health plan in a standard transaction.

(3) Communicate to the Enumeration System any changes in its required data elements in the Enumeration System within 30 days of the change.

(b) A controlling health plan may do the following:

(1) Obtain an HPID from the Enumeration System for a subhealth plan of the controlling health plan.

(2) Direct a subhealth plan of the controlling health plan to obtain an HPID from the Enumeration System.

(c) A subhealth plan may obtain an HPID from the Enumeration System.

(d) A subhealth plan that is assigned an HPID from the Enumeration System must comply with the requirements that apply to a controlling health plan in paragraphs (a)(2) and (a)(3) of this section.



**§ 162.514 Other entity identifier.**

(a) An entity may obtain an Other Entity Identifier (OEID) to identify itself if the entity meets all of the following:

(1) Needs to be identified in a transaction for which the Secretary has adopted a standard under this part.

(2) Is not eligible to obtain an HPID.

(3) Is not eligible to obtain an NPI.

(4) Is not an individual.

(b) An OEID must be obtained from the Enumeration System identified in § 162.508.

(c) *Uses for the OEID.* (1) An other entity may use the OEID it obtained from the Enumeration System to identify itself or have itself identified on all covered transactions in which it needs to be identified.

(2) The OEID may be used for any other lawful purpose.

**Subpart F—Standard Unique Employer Identifier**

SOURCE: 67 FR 38020, May 31, 2002, unless otherwise noted.

**§ 162.600 Compliance dates of the implementation of the standard unique employer identifier.**

(a) *Health care providers.* Health care providers must comply with the requirements of this subpart no later than July 30, 2004.

(b) *Health plans.* A health plan must comply with the requirements of this subpart no later than one of the following dates:

(1) *Health plans other than small health plans* —July 30, 2004.

(2) *Small health plans* —August 1, 2005.

(c) *Health care clearinghouses.* Health care clearinghouses must comply with the requirements of this subpart no later than July 30, 2004.

**§ 162.605 Standard unique employer identifier.**

The Secretary adopts the EIN as the standard unique employer identifier provided for by 42 U.S.C. 1320d-2(b).

**§ 162.610 Implementation specifications for covered entities.**

(a) The standard unique employer identifier of an employer of a particular employee is the EIN that appears on that employee's IRS Form W-2, Wage and Tax Statement, from the employer.

(b) A covered entity must use the standard unique employer identifier (EIN) of the appropriate employer in standard transactions that require an employer identifier to identify a person or entity as an employer, including where situationally required.

(c) Required and permitted uses for the Employer Identifier.

(1) The Employer Identifier must be used as stated in § 162.610(b).

(2) The Employer Identifier may be used for any other lawful purpose.

[67 FR 38020, May 31, 2002, as amended at 69 FR 3469, Jan. 23, 2004]

**Subparts G-H [Reserved]**

**Subpart I—General Provisions for Transactions**

**§ 162.900 [Reserved]**

**§ 162.910 Maintenance of standards and adoption of modifications and new standards.**

(a) *Designation of DSMOs.* (1) The Secretary may designate as a DSMO an organization that agrees to conduct, to the satisfaction of the Secretary, the following functions:

(i) Maintain standards adopted under this subchapter.

(ii) Receive and process requests for adopting a new standard or modifying an adopted standard.

(2) The Secretary designates a DSMO by notice in the FEDERAL REGISTER.

(b) *Maintenance of standards.* Maintenance of a standard by the appropriate DSMO constitutes maintenance of the standard for purposes of this part, if done in accordance with the processes the Secretary may require.

(c) *Process for modification of existing standards and adoption*

*of new standards.* The Secretary considers a recommendation for a proposed modification to an existing standard, or a proposed new standard, only if the recommendation is developed through a process that provides for the following:

- (1) Open public access.
- (2) Coordination with other DSMOs.
- (3) An appeals process for each of the following, if dissatisfied with the decision on the request:
  - (i) The requestor of the proposed modification.
  - (ii) A DSMO that participated in the review and analysis of the request for the proposed modification, or the proposed new standard.
- (4) Expedited process to address content needs identified within the industry, if appropriate.
- (5) Submission of the recommendation to the National Committee on Vital and Health Statistics (NCVHS).

**§ 162.915 Trading partner agreements.**

A covered entity must not enter into a trading partner agreement that would do any of the following:

- (a) Change the definition, data condition, or use of a data element or segment in a standard or operating rule, except where necessary to implement State or Federal law, or to protect against fraud and abuse.

- (b) Add any data elements or segments to the maximum defined data set.

- (c) Use any code or data elements that are either marked “not used” in the standard's implementation specification or are not in the standard's implementation specification(s).

- (d) Change the meaning or intent of the standard's implementation specification(s).

[65 FR 50367, Aug. 17, 2000, as amended at 76 FR 40495, July 8, 2011]

**§ 162.920 Availability of implementation specifications and operating rules.**

Certain material is incorporated by reference into this subpart with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in this section, the Department of Health and Human Services must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. All approved material is available for inspection at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call (202) 714-6030, or go to: [http://www.archives.gov/federal\\_register/code\\_of\\_federal\\_regulations/ibr\\_locations.html](http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html). The materials are also available for inspection by the public at the Centers for Medicare & Medicaid Services (CMS), 7500 Security Boulevard, Baltimore, Maryland 21244. For more information on the availability on the materials at CMS, call (410) 786-6597. The materials

are also available from the sources listed below.

(a) *ASC X12N specifications and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3.* The implementation specifications for the ASC X12N and the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3 (and accompanying Errata or Type 1 Errata) may be obtained from the ASC X12, 7600 Leesburg Pike, Suite 430, Falls Church, VA 22043; Telephone (703) 970-4480; and FAX (703) 970-4488. They are also available through the internet at <http://www.X12.org>. A fee is charged for all implementation specifications, including Technical Reports Type 3. Charging for such publications is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1, as referenced in § 162.1102 and § 162.1802.

(2) The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1, as referenced in § 162.1102 and § 162.1802.

(3) The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1 as referenced in § 162.1102 and § 162.1802.

(4) The ASC X12N 835—Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, and Addenda to Health Care Claim Payment/Advice, Version 4010, October 2002, Washington Publishing Company, 004010X091A1 as referenced in § 162.1602.

(5) ASC X12N 834—Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 and Addenda to Benefit Enrollment and Maintenance, Version 4010, October 2002, Washington Publishing Company, 004010X095A1, as referenced in § 162.1502.

(6) The ASC X12N 820—Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, and Addenda to Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, October 2002, Washington Publishing Company, 004010X061A1, as referenced in § 162.1702.

(7) The ASC X12N 278—Health Care Services Review—

Request for Review and Response, Version 4010, May 2000, Washington Publishing Company, 004010X094 and Addenda to Health Care Services Review—Request for Review and Response, Version 4010, October 2002, Washington Publishing Company, 004010X094A1, as referenced in § 162.1302.

(8) The ASC X12N-276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 and Addenda to Health Care Claim Status Request and Response, Version 4010, October 2002, Washington Publishing Company, 004010X093A1, as referenced in § 162.1402.

(9) The ASC X12N 270/271—Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, Washington Publishing Company, 004010X092A1, as referenced in § 162.1202.

(10) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim Dental (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1, as referenced in § 162.1102 and § 162.1802.

(11) The ASC X12 Standards for Electronic Data Interchange

Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12, 005010X222, as referenced in § 162.1102 and § 162.1802.

(12) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12/N005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1, as referenced in § 162.1102 and § 162.1802.

(13) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221, as referenced in § 162.1602.

(14) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220, as referenced in § 162.1502.

(15) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007, ASC X12N/005010X218, as referenced in § 162.1702.

(16) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Services Review—Request for Review and Response (278), May 2006, ASC X12N/005010X217, and Errata to Health Care Services

Review—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1, as referenced in § 162.1302.

(17) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1, as referenced in § 162.1402.

(18) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279, as referenced in § 162.1202.

(b) *Retail pharmacy specifications and Medicaid subrogation implementation guides.* The implementation specifications for the retail pharmacy standards and the implementation specifications for the batch standard for the Medicaid pharmacy subrogation transaction may be obtained from the National Council for Prescription Drug Programs, 9240 East Raintree Drive, Scottsdale, AZ 85260. Telephone (480) 477-1000; FAX (480) 767-1042. They are also available through the Internet at <http://www.ncdp.org>. A fee is charged for all NCPDP Implementation Guides. Charging for such publications

is consistent with the policies of other publishers of standards. The transaction implementation specifications are as follows:

(1) The Telecommunication Standard Implementation Guide Version 5, Release 1 (Version 5.1), September 1999, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, § 162.1602, and § 162.1802.

(2) The Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(3) The National Council for Prescription Drug Programs (NCPDP) equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 0, February 1, 1996, as referenced in § 162.1102, § 162.1202, § 162.1602, and § 162.1802.

(4) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, National Council for Prescription Drug Programs, as referenced in § 162.1102, § 162.1202, § 162.1302, and § 162.1802.

(5) The Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), January 2006, National Council for Prescription Drug Programs, as referenced in § 162.1102,

§ 162.1202, § 162.1302, and § 162.1802.

(6) The Batch Standard Medicaid Subrogation Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902.

(c) Council for Affordable Quality Healthcare's (CAQH) Committee on Operating Rules for Information Exchange (CORE), 601 Pennsylvania Avenue, NW. South Building, Suite 500 Washington, DC 20004; Telephone (202) 861-1492; Fax (202) 861-1454; E-mail [info@CAQH.org](mailto:info@CAQH.org); and Internet at <http://www.caqh.org/benefits.php>.

(1) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase I Policies and Operating Rules, Approved April 2006, v5010 Update March 2011.

(i) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(ii) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase I CORE 155: Eligibility and Benefits Batch Response Time Rule, version

1.1.0, March 2011, as referenced in § 162.1203.

(v) Phase I CORE 156: Eligibility and Benefits Real Time Response Time Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(vi) Phase I CORE 157: Eligibility and Benefits System Availability Rule, version 1.1.0, March 2011, as referenced in § 162.1203.

(2) ACME Health Plan, HIPAA Transaction Standard Companion Guide, Refers to the Implementation Guides Based on ASC X12 version 005010, CORE v5010 Master Companion Guide Template, 005010, 1.2, (CORE v 5010 Master Companion Guide Template, 005010, 1.2), March 2011, as referenced in §§ 162.1203, 162.1403, and 162.1603.

(3) CAQH, Committee on Operating Rules for Information Exchange, CORE Phase II Policies and Operating Rules, Approved July 2008, v5010 Update March 2011.

(i) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, as referenced in § 162.1403.

(ii) Phase II CORE 258: Eligibility and Benefits 270/271 Normalizing Patient Last Name Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iii) Phase II CORE 259: Eligibility and Benefits 270/271 AAA Error Code Reporting Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(iv) Phase II CORE 260: Eligibility & Benefits Data Content (270/271) Rule, version 2.1.0, March 2011, as referenced in § 162.1203.

(v) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011, as referenced in § 162.1203 and § 162.1403.

(4) Council for Affordable Quality Healthcare (CAQH) Phase III Committee on Operating Rules for Information Exchange (CORE) EFT & ERA Operating Rule Set, Approved June 2012, as specified in this paragraph and referenced in § 162.1603.

(i) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(ii) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(iii) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(iv) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(v) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(vi) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled “Health Care Claim Payment/Advice

Batch Acknowledgement Requirements”.

(d) The National Automated Clearing House Association (NACHA), The Electronic Payments Association, 1350 Sunrise Valley Drive, Suite 100, Herndon, Virginia 20171 (Phone) (703) 561-1100; (Fax) (703) 713-1641; Email: [info@nacha.org](mailto:info@nacha.org); and Internet at <http://www.nacha.org>. The implementation specifications are as follows:

(1) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules, Appendix One: ACH File Exchange Specifications (Operating Rule 59) as referenced in § 162.1602.

(2) 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network, NACHA Operating Rules Appendix Three: ACH Record Format Specifications (Operating Rule 78), Part 3.1, Subpart 3.1.8 Sequence of Records for CCD Entries as referenced in § 162.1602.

[68 FR 8396, Feb. 20, 2003, as amended at 69 FR 18803, Apr. 9, 2004; 74 FR 3324, Jan. 16, 2009; 76 FR 40495, July 8, 2011; 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

#### **§ 162.923 Requirements for covered entities.**

(a) *General rule.* Except as otherwise provided in this part, if a covered entity conducts, with another covered entity that is required to comply with a transaction standard adopted

under this part (or within the same covered entity), using electronic media, a transaction for which the Secretary has adopted a standard under this part, the covered entity must conduct the transaction as a standard transaction.

(b) *Exception for direct data entry transactions.* A health care provider electing to use direct data entry offered by a health plan to conduct a transaction for which a standard has been adopted under this part must use the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard.

(c) *Use of a business associate.* A covered entity may use a business associate, including a health care clearinghouse, to conduct a transaction covered by this part. If a covered entity chooses to use a business associate to conduct all or part of a transaction on behalf of the covered entity, the covered entity must require the business associate to do the following:

- (1) Comply with all applicable requirements of this part.
- (2) Require any agent or subcontractor to comply with all applicable requirements of this part.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

#### **§ 162.925 Additional requirements for health plans.**

(a) *General rules.* (1) If an entity requests a health plan to conduct

a transaction as a standard transaction, the health plan must do so.

(2) A health plan may not delay or reject a transaction, or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction.

(3) A health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).

(4) A health plan may not offer an incentive for a health care provider to conduct a transaction covered by this part as a transaction described under the exception provided for in § 162.923(b).

(5) A health plan that operates as a health care clearinghouse, or requires an entity to use a health care clearinghouse to receive, process, or transmit a standard transaction may not charge fees or costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard transaction to, or from, a health plan.

(6) During the period from March 17, 2009 through December 31, 2011, a health plan may not delay or reject a standard transaction, or attempt to adversely affect the other entity or the transaction, on the basis that it does not comply with another adopted standard for the same period.

(b) *Coordination of benefits.* If a health plan receives a standard transaction and coordinates

benefits with another health plan (or another payer), it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan (or other payer).

(c) *Code sets.* A health plan must meet each of the following requirements:

(1) Accept and promptly process any standard transaction that contains codes that are valid, as provided in subpart J of this part.

(2) Keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

[65 FR 50367, Aug. 17, 2000, as amended at 74 FR 3325, Jan. 16, 2009]

#### **§ 162.930 Additional rules for health care clearinghouses.**

When acting as a business associate for another covered entity, a health care clearinghouse may perform the following functions:

(a) Receive a standard transaction on behalf of the covered entity and translate it into a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) for transmission to the covered entity.

(b) Receive a nonstandard transaction (for example, nonstandard format and/or nonstandard data content) from the covered entity and translate it into a standard transaction for transmission on behalf of the covered entity.

**§ 162.940 Exceptions from standards to permit testing of proposed modifications.**

*(a) Requests for an exception.*

An organization may request an exception from the use of a standard from the Secretary to test a proposed modification to that standard. For each proposed modification, the organization must meet the following requirements:

(1) *Comparison to a current standard.* Provide a detailed explanation, no more than 10 pages in length, of how the proposed modification would be a significant improvement to the current standard in terms of the following principles:

(i) Improve the efficiency and effectiveness of the health care system by leading to cost reductions for, or improvements in benefits from, electronic health care transactions.

(ii) Meet the needs of the health data standards user community, particularly health care providers, health plans, and health care clearinghouses.

(iii) Be uniform and consistent with the other standards adopted under this part and, as appropriate, with other private and public sector health data standards.

(iv) Have low additional development and implementation costs relative to the benefits of using the standard.

(v) Be supported by an ANSI-accredited SSO or other private or public organization that would maintain the standard over time.

(vi) Have timely development, testing, implementation, and updating procedures to achieve administrative simplification benefits faster.

(vii) Be technologically independent of the computer platforms and transmission protocols used in electronic health transactions, unless they are explicitly part of the standard.

(viii) Be precise, unambiguous, and as simple as possible.

(ix) Result in minimum data collection and paperwork burdens on users.

(x) Incorporate flexibility to adapt more easily to changes in the health care infrastructure (such as new services, organizations, and provider types) and information technology.

(2) *Specifications for the proposed modification.* Provide specifications for the proposed modification, including any additional system requirements.

(3) *Testing of the proposed modification.* Provide an explanation, no more than 5 pages in length, of how the organization intends to test the standard, including the number and types of health plans and health care providers expected to be involved in the test, geographical areas, and beginning and ending dates of the test.

(4) *Trading partner concurrences.* Provide written concurrences from trading partners who would agree to participate in the test.

(b) *Basis for granting an exception.* The Secretary may grant an initial exception, for a period not to exceed 3 years, based on, but not limited to, the following criteria:

(1) An assessment of whether the proposed modification demonstrates a significant improvement to the current standard.

(2) The extent and length of time of the exception.

(3) Consultations with DSMOs.

(c) *Secretary's decision on exception.* The Secretary makes a decision and notifies the organization requesting the exception whether the request is granted or denied.

(1) *Exception granted.* If the Secretary grants an exception, the notification includes the following information:

(i) The length of time for which the exception applies.

(ii) The trading partners and geographical areas the Secretary approves for testing.

(iii) Any other conditions for approving the exception.

(2) *Exception denied.* If the Secretary does not grant an exception, the notification explains the reasons the Secretary considers the proposed modification would not be a significant improvement to the current standard and any other rationale for the denial.

(d) *Organization's report on test results.* Within 90 days after the test is completed, an organization that receives an

exception must submit a report on the results of the test, including a cost-benefit analysis, to a location specified by the Secretary by notice in the FEDERAL REGISTER.

(e) *Extension allowed.* If the report submitted in accordance with paragraph (d) of this section recommends a modification to the standard, the Secretary, on request, may grant an extension to the period granted for the exception.

## Subpart J—Code Sets

### § 162.1000 General requirements.

When conducting a transaction covered by this part, a covered entity must meet the following requirements:

(a) *Medical data code sets.* Use the applicable medical data code sets described in § 162.1002 as specified in the implementation specification adopted under this part that are valid at the time the health care is furnished.

(b) *Nonmedical data code sets.* Use the nonmedical data code sets as described in the implementation specifications adopted under this part that are valid at the time the transaction is initiated.

### § 162.1002 Medical data code sets.

The Secretary adopts the following maintaining organization's code sets as the standard medical data code sets:

(a) For the period from October 16, 2002 through October 15, 2003:

(1) *International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

(i) Diseases.

(ii) Injuries.

(iii) Impairments.

(iv) Other health problems and their manifestations.

(v) Causes of injury, disease, impairment, or other health problems.

(2) *International Classification of Diseases, 9th Edition, Clinical Modification, Volume 3 Procedures* (including The Official ICD-9-CM Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

(i) Prevention.

(ii) Diagnosis.

(iii) Treatment.

(iv) Management.

(3) *National Drug Codes (NDC)*, as maintained and distributed by HHS, in collaboration with drug manufacturers, for the following:

(i) Drugs

(ii) Biologics.

(4) *Code on Dental Procedures and Nomenclature*, as maintained and distributed by the American Dental Association, for dental services.

(5) The combination of *Health Care Financing Administration Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, and *Current Procedural Terminology, Fourth Edition (CPT-4)*, as maintained and distributed by the American Medical Association, for physician services and other health care services. These services include, but are not limited to, the following:

(i) Physician services.

(ii) Physical and occupational therapy services.

(iii) Radiologic procedures.

(iv) Clinical laboratory tests.

(v) Other medical diagnostic procedures.

(vi) Hearing and vision services.

(vii) Transportation services including ambulance.

(6) The *Health Care Financing Administration Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services. These items include, but are not limited to, the following:

(i) Medical supplies.



- (ii) Orthotic and prosthetic devices.
- (iii) Durable medical equipment.

(b) For the period on and after October 16, 2003 through September 30, 2014:

(1) The code sets specified in paragraphs (a)(1), (a)(2), (a)(4), and (a)(5) of this section.

(2) *National Drug Codes (NDC)*, as maintained and distributed by HHS, for reporting the following by retail pharmacies:

- (i) Drugs.
- (ii) Biologics.

(3) *The Healthcare Common Procedure Coding System (HCPCS)*, as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services, with the exception of drugs and biologics. These items include, but are not limited to, the following:

- (i) Medical supplies.
- (ii) Orthotic and prosthetic devices.
- (iii) Durable medical equipment.

(c) For the period on and after October 1, 2014:

(1) The code sets specified in paragraphs (a)(4), (a)(5), (b)(2), and (b)(3) of this section.

(2) International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM) (including The Official ICD-10-CM Guidelines for

Coding and Reporting), as maintained and distributed by HHS, for the following conditions:

- (i) Diseases.
- (ii) Injuries.
- (iii) Impairments.
- (iv) Other health problems and their manifestations.

(v) Causes of injury, disease, impairment, or other health problems.

(3) International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS) (including The Official ICD-10-PCS Guidelines for Coding and Reporting), as maintained and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

- (i) Prevention.
- (ii) Diagnosis.
- (iii) Treatment.
- (iv) Management.

[65 FR 50367, Aug. 17, 2000, as amended at 68 FR 8397, Feb. 20, 2003; 74 FR 3362, Jan. 16, 2009; 77 FR 54720, Sept. 5, 2012]

#### **§ 162.1011 Valid code sets.**

Each code set is valid within the dates specified by the organization responsible for maintaining that code set.

### **Subpart K—Health Care Claims or Equivalent Encounter Information**

#### **§ 162.1101 Health care claims or equivalent encounter information transaction.**

The health care claims or equivalent encounter information transaction is the transmission of either of the following:

(a) A request to obtain payment, and the necessary accompanying information from a health care provider to a health plan, for health care.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

#### **§ 162.1102 Standards for health care claims or equivalent encounter information transaction.**

The Secretary adopts the following standards for the health care claims or equivalent encounter information transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs claims.* The National Council for Prescription Drug Programs (NCPDP) Telecommunication Standards Implementation Guide, Version 5, Release 1, September 1999, and equivalent NCPDP Batch Standards Batch Implementation Guide, Version

1, Release 1, (Version 1.1), January 2000, supporting Telecommunication Version 5.1 for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, health care claims.* The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097. and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims.* The ASC X12N 837—Health Care Claims: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claims: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010x098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims.* The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1)(i) The standards identified in paragraph (a) of this section; and

(ii) For retail pharmacy supplies and professional services claims, the following: The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096, October 2002 (Incorporated by reference in § 162.920); and

(2)(i) *Retail pharmacy drug claims.* The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007 and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837) ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) *Professional health care claims.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(iv) *Institutional health care claims.* The ASC X12 Standards

for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837) ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(v) *Retail pharmacy supplies and professional services claims.* (A) The Telecommunication Standard, Implementation Guide Version 5, Release 1, September 1999. (Incorporated by reference in § 162.920.)

(B) The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs (Incorporated by reference in § 162.920); and

(C) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222. (Incorporated by reference in § 162.920.)

(c) For the period on and after the January 1, 2012, the standards identified in paragraph (b)(2) of this section, except the standard identified in paragraph (b)(2)(v)(A) of this section.

[68 FR 8397, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3325, Jan. 16, 2009]

**Subpart L—Eligibility for a Health Plan**

**§ 162.1201 Eligibility for a health plan transaction.**

The eligibility for a health plan transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan, or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

(1) Eligibility to receive health care under the health plan.

(2) Coverage of health care under the health plan.

(3) Benefits associated with the benefit plan.

(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.

**§ 162.1202 Standards for eligibility for a health plan transaction.**

The Secretary adopts the following standards for the eligibility for a health plan transaction:

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drugs.* The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch

Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000 supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental, professional, and institutional health care eligibility benefit inquiry and response.* The ASC X12N 270/271—Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 and Addenda to Health Care Eligibility Benefit Inquiry and Response, Version 4010, October 2002, Washington Publishing Company, 004010X092A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011 both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs.* The Telecommunication Standard Implementation Guide Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) *Dental, professional, and institutional health care eligibility benefit inquiry and response.* The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Eligibility

Benefit Inquiry and Response (270/271), April 2008, ASC X12N/005010X279. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003; 68 FR 11445, Mar. 10, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

**§ 162.1203 Operating rules for eligibility for a health plan transaction.**

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase I and Phase II operating rules (updated for Version 5010) for the eligibility for a health plan transaction:

(1) Phase I CORE 152: Eligibility and Benefit Real Time Companion Guide Rule, version 1.1.0, March 2011, and CORE v5010 Master Companion Guide Template. (Incorporated by reference in § 162.920).

(2) Phase I CORE 153: Eligibility and Benefits Connectivity Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(3) Phase I CORE 154: Eligibility and Benefits 270/271 Data Content Rule, version 1.1.0, March 2011. (Incorporated by reference in § 162.920).

(4) Phase I CORE 155:  
Eligibility and Benefits Batch  
Response Time Rule, version  
1.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(5) Phase I CORE 156:  
Eligibility and Benefits Real  
Time Response Rule, version  
1.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(6) Phase I CORE 157:  
Eligibility and Benefits System  
Availability Rule, version 1.1.0,  
March 2011. (Incorporated by  
reference in § 162.920).

(7) Phase II CORE 258:  
Eligibility and Benefits 270/271  
Normalizing Patient Last Name  
Rule, version 2.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(8) Phase II CORE 259:  
Eligibility and Benefits 270/271  
AAA Error Code Reporting  
Rule, version 2.1.0.  
(Incorporated by reference in  
§ 162.920).

(9) Phase II CORE 260:  
Eligibility & Benefits Data  
Content (270/271) Rule, version  
2.1.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(10) Phase II CORE 270:  
Connectivity Rule, version  
2.2.0, March 2011.  
(Incorporated by reference in  
§ 162.920).

(b) Excluding where the CAQH  
CORE rules reference and  
pertain to acknowledgements  
and CORE certification.

[76 FR 40496, July 8, 2011]

#### **Subpart M—Referral Certification and Authorization**

##### **§ 162.1301 Referral certification and authorization transaction.**

The referral certification and  
authorization transaction is any  
of the following transmissions:

(a) A request from a health care  
provider to a health plan for the  
review of health care to obtain  
an authorization for the health  
care.

(b) A request from a health care  
provider to a health plan to  
obtain authorization for referring  
an individual to another health  
care provider.

(c) A response from a health  
plan to a health care provider to  
a request described in paragraph  
(a) or paragraph (b) of this  
section.

[74 FR 3326, Jan. 16, 2009]

##### **§ 162.1302 Standards for referral certification and authorization transaction.**

The Secretary adopts the  
following standards for the  
referral certification and  
authorization transaction:

(a) For the period from October  
16, 2003 through March 16,  
2009:

(1) *Retail pharmacy drug  
referral certification and  
authorization.* The NCPDP  
Telecommunication Standard  
Implementation Guide, Version  
5, Release 1 (Version 5.1),  
September 1999, and equivalent  
NCPDP Batch Standard Batch  
Implementation Guide, Version

1, Release 1 (Version 1.1),  
January 2000, supporting  
Telecommunications Standard  
Implementation Guide, Version  
5, Release 1 (Version 5.1) for  
the NCPDP Data Record in the  
Detail Data Record.  
(Incorporated by reference in  
§ 162.920).

(2) *Dental, professional, and  
institutional referral  
certification and authorization.*  
The ASC X12N 278—Health  
Care Services Review—Request  
for Review and Response,  
Version 4010, May 2000,  
Washington Publishing  
Company, 004010X094 and  
Addenda to Health Care  
Services Review—Request for  
Review and Response, Version  
4010, October 2002,  
Washington Publishing  
Company, 004010X094A1.  
(Incorporated by reference in  
§ 162.920).

(b) For the period from March  
17, 2009 through December 31,  
2011 both—

(1) The standards identified in  
paragraph (a) of this section; and

(2)(i) *Retail pharmacy drugs.*  
The Telecommunication  
Standard Implementation Guide  
Version D, Release 0 (Version  
D.0), August 2007, and  
equivalent Batch Standard  
Implementation Guide, Version  
1, Release 2 (Version 1.2),  
National Council for  
Prescription Drug Programs.  
(Incorporated by reference in  
§ 162.920.)

(ii) *Dental, professional, and  
institutional request for review  
and response.* The ASC X12  
Standards for Electronic Data  
Interchange Technical Report  
Type 3—Health Care Services  
Review—Request for Review

and Response (278), May 2006, ASC X12N/005010X217, and Errata to Health Care Services Review—Request for Review and Response (278), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X217E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8398, Feb. 20, 2003, as amended at 74 FR 3326, Jan. 16, 2009]

#### **Subpart N—Health Care Claim Status**

##### **§ 162.1401 Health care claim status transaction.**

The health care claim status transaction is the transmission of either of the following:

(a) An inquiry from a health care provider to a health plan to determine the status of a health care claim.

(b) A response from a health plan to a health care provider about the status of a health care claim.

[74 FR 3326, Jan. 16, 2009]

##### **§ 162.1402 Standards for health care claim status transaction.**

The Secretary adopts the following standards for the health care claim status transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N-276/277 Health Care Claim Status Request and Response, Version 4010, May 2000, Washington Publishing Company, 004010X093 and Addenda to Health Care Claim Status Request and Response, Version 4010, October 2002, Washington Publishing Company, 004010X093A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Status Request and Response (276/277), August 2006, ASC X12N/005010X212, and Errata to Health Care Claim Status Request and Response (276/277), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, April 2008, ASC X12N/005010X212E1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3326, Jan. 16, 2009]

##### **§ 162.1403 Operating rules for health care claim status transaction.**

On and after January 1, 2013, the Secretary adopts the following:

(a) Except as specified in paragraph (b) of this section, the following CAQH CORE Phase II operating rules (updated for Version 5010) for the health care claim status transaction:

(1) Phase II CORE 250: Claim Status Rule, version 2.1.0, March 2011, and CORE v5010 Master Companion Guide, 00510, 1.2, March 2011. (Incorporated by reference in § 162.920).

(2) Phase II CORE 270: Connectivity Rule, version 2.2.0, March 2011. (Incorporated by reference in § 162.920).

(b) Excluding where the CAQH CORE rules reference and pertain to acknowledgements and CORE certification.

[76 FR 40496, July 8, 2011]

#### **Subpart O—Enrollment and Disenrollment in a Health Plan**

##### **§ 162.1501 Enrollment and disenrollment in a health plan transaction.**

The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information from the sponsor of the insurance coverage, benefits, or policy, to a health plan to establish or terminate insurance coverage.

[74 FR 3327, Jan. 16, 2009]

##### **§ 162.1502 Standards for enrollment and disenrollment in a health plan transaction.**

The Secretary adopts the following standards for

enrollment and disenrollment in a health plan transaction.

(a) For the period from October 16, 2003 through March 16, 2009: ASC X12N 834—Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 and Addenda to Benefit Enrollment and Maintenance, Version 4010, October 2002, Washington Publishing Company, 004010X095A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section; and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Benefit Enrollment and Maintenance (834), August 2006, ASC X12N/005010X220 (Incorporated by reference in § 162.920)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

**Subpart P—Health Care Electronic Funds Transfers (EFT) and Remittance Advice**

**§ 162.1601 Health care electronic funds transfers (EFT) and remittance advice transaction.**

The health care electronic funds transfers (EFT) and remittance advice transaction is the transmission of either of the following for health care:

(a) The transmission of any of the following from a health plan to a health care provider:

(1) Payment.

(2) Information about the transfer of funds.

(3) Payment processing information.

(b) The transmission of either of the following from a health plan to a health care provider:

(1) Explanation of benefits.

(2) Remittance advice.

[65 FR 50367, Aug. 17, 2000, as amended at 77 FR 1590, Jan. 10, 2012; 77 FR 48043, Aug. 10, 2012]

**§ 162.1602 Standards for health care electronic funds transfers (EFT) and remittance advice transaction.**

The Secretary adopts the following standards:

(a) For the period from October 16, 2003 through March 16, 2009: Health care claims and remittance advice. The ASC X12N 835—Health Care Claim Payment/Advice, Version 4010, May 2000, Washington Publishing Company, 004010X091, and Addenda to Health Care Claim Payment/Advice, Version 4010, October 2002, Washington Publishing Company, 004010X091A1. (Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both of the following standards:

(1) The standard identified in paragraph (a) of this section.

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920.)

(c) For the period from January 1, 2012 through December 31, 2013, the standard identified in paragraph (b)(2) of this section.

(d) For the period on and after January 1, 2014, the following standards:

(1) Except when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, for Stage 1 Payment Initiation transmissions described in § 162.1601(a), all of the following standards:

(i) The National Automated Clearing House Association (NACHA) Corporate Credit or Deposit Entry with Addenda Record (CCD+) implementation specifications as contained in the 2011 NACHA Operating Rules & Guidelines, A Complete Guide to the Rules Governing the ACH Network as follows (incorporated by reference in § 162.920)—

(A) NACHA Operating Rules, Appendix One: ACH File Exchange Specifications; and

(B) NACHA Operating Rules, Appendix Three: ACH Record Format Specifications, Subpart 3.1.8 Sequence of Records for CCD Entries.

(ii) For the CCD Addenda Record (“7”), field 3, of the

standard identified in 1602(d)(1)(i), the Accredited Standards Committee (ASC) X12 Standards for Electronic Data Interchange Technical Report Type 3, “Health Care Claim Payment/Advice (835), April 2006: Section 2.4: 835 Segment Detail: “TRN Reassociation Trace Number,” Washington Publishing Company, 005010X221 (Incorporated by reference in § 162.920).

(2) For transmissions described in § 162.1601(b), including when transmissions as described in § 162.1601(a) and (b) are contained within the same transmission, the ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, “Health Care Claim Payment/Advice (835), April 2006, ASC X12N/005010X221. (Incorporated by reference in § 162.920).

[77 FR 1590, Jan. 10, 2012]

**§ 162.1603 Operating rules for health care electronic funds transfers (EFT) and remittance advice transaction.**

On and after January 1, 2014, the Secretary adopts the following for the health care electronic funds transfers (EFT) and remittance advice transaction:

(a) The Phase III CORE EFT & ERA Operating Rule Set, Approved June 2012 (Incorporated by reference in § 162.920) which includes the following rules:

(1) Phase III CORE 380 EFT Enrollment Data Rule, version 3.0.0, June 2012.

(2) Phase III CORE 382 ERA Enrollment Data Rule, version 3.0.0, June 2012.

(3) Phase III 360 CORE Uniform Use of CARCs and RARCs (835) Rule, version 3.0.0, June 2012.

(4) CORE-required Code Combinations for CORE-defined Business Scenarios for the Phase III CORE 360 Uniform Use of Claim Adjustment Reason Codes and Remittance Advice Remark Codes (835) Rule, version 3.0.0, June 2012.

(5) Phase III CORE 370 EFT & ERA Reassociation (CCD+/835) Rule, version 3.0.0, June 2012.

(6) Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012, except Requirement 4.2 titled “Health Care Claim Payment/Advice Batch Acknowledgement Requirements”.

(b) ACME Health Plan, CORE v5010 Master Companion Guide Template, 005010, 1.2, March 2011 (incorporated by reference in § 162.920), as required by the Phase III CORE 350 Health Care Claim Payment/Advice (835) Infrastructure Rule, version 3.0.0, June 2012.

[77 FR 48043, Aug. 10, 2012]

**Subpart Q—Health Plan Premium Payments**

**§ 162.1701 Health plan premium payments transaction.**

The health plan premium payment transaction is the transmission of any of the

following from the entity that is arranging for the provision of health care or is providing health care coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit health care premium payments including any of the following:

(1) Payroll deductions.

(2) Other group premium payments.

(3) Associated group premium payment information.

**§ 162.1702 Standards for health plan premium payments transaction.**

The Secretary adopts the following standards for the health plan premium payments transaction:

(a) For the period from October 16, 2003 through March 16, 2009: The ASC X12N 820—Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061, and Addenda to Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, October 2002, Washington Publishing Company, 004010X061A1.

(Incorporated by reference in § 162.920.)

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standard identified in paragraph (a) of this section, and

(2) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Payroll Deducted and Other Group Premium Payment for Insurance Products (820), February 2007, ASC X12N/005010X218. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standard identified in paragraph (b)(2) of this section.

[74 FR 3327, Jan. 16, 2009]

## **Subpart R—Coordination of Benefits**

### **§ 162.1801 Coordination of benefits transaction.**

The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for health care:

(a) Claims.

(b) Payment information.

### **§ 162.1802 Standards for coordination of benefits information transaction.**

The Secretary adopts the following standards for the

coordination of benefits information transaction.

(a) For the period from October 16, 2003 through March 16, 2009:

(1) *Retail pharmacy drug claims.* The National Council for Prescription Drug Programs Telecommunication Standard Implementation Guide, Version 5, Release 1 (Version 5.1), September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1, Release 1 (Version 1.1), January 2000, supporting Telecommunications Standard Implementation Guide, Version 5, Release 1 (Version 5.1) for the NCPDP Data Record in the Detail Data Record. (Incorporated by reference in § 162.920).

(2) *Dental health care claims.* The ASC X12N 837—Health Care Claim: Dental, Version 4010, May 2000, Washington Publishing Company, 004010X097 and Addenda to Health Care Claim: Dental, Version 4010, October 2002, Washington Publishing Company, 004010X097A1. (Incorporated by reference in § 162.920).

(3) *Professional health care claims.* The ASC X12N 837—Health Care Claim: Professional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X098 and Addenda to Health Care Claim: Professional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X098A1. (Incorporated by reference in § 162.920).

(4) *Institutional health care claims.* The ASC X12N 837—Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, May 2000, Washington Publishing Company, 004010X096 and Addenda to Health Care Claim: Institutional, Volumes 1 and 2, Version 4010, October 2002, Washington Publishing Company, 004010X096A1. (Incorporated by reference in § 162.920).

(b) For the period from March 17, 2009 through December 31, 2011, both:

(1) The standards identified in paragraph (a) of this section; and

(2)(i) *Retail pharmacy drug claims.* The Telecommunication Standard Implementation Guide, Version D, Release 0 (Version D.0), August 2007, and equivalent Batch Standard Implementation Guide, Version 1, Release 2 (Version 1.2), National Council for Prescription Drug Programs. (Incorporated by reference in § 162.920.)

(ii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Dental (837), May 2006, ASC X12N/005010X224, and Type 1 Errata to Health Care Claim: Dental (837), ASC X12 Standards for Electronic Date Interchange Technical Report Type 3, October 2007, ASC X12N/005010X224A1. (Incorporated by reference in § 162.920.)

(iii) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Professional (837), May 2006, ASC X12N/005010X222.



(Incorporated by reference in § 162.920.)

(iv) The ASC X12 Standards for Electronic Data Interchange Technical Report Type 3—Health Care Claim: Institutional (837), May 2006, ASC X12N/005010X223, and Type 1 Errata to Health Care Claim: Institutional (837), ASC X12 Standards for Electronic Data Interchange Technical Report Type 3, October 2007, ASC X12N/005010X223A1. (Incorporated by reference in § 162.920.)

(c) For the period on and after January 1, 2012, the standards identified in paragraph (b)(2) of this section.

[68 FR 8399, Feb. 20, 2003, as amended at 74 FR 3327, Jan. 16, 2009]

#### **Subpart S—Medicaid Pharmacy Subrogation**

SOURCE: 74 FR 3328, Jan. 16, 2009, unless otherwise noted.

#### **§ 162.1901 Medicaid pharmacy subrogation transaction.**

The Medicaid pharmacy subrogation transaction is the transmission of a claim from a Medicaid agency to a payer for the purpose of seeking reimbursement from the responsible health plan for a pharmacy claim the State has paid on behalf of a Medicaid recipient.

#### **§ 162.1902 Standard for Medicaid pharmacy subrogation transaction.**

The Secretary adopts the Batch Standard Medicaid Subrogation

Implementation Guide, Version 3, Release 0 (Version 3.0), July 2007, National Council for Prescription Drug Programs, as referenced in § 162.1902 (Incorporated by reference at § 162.920):

(a) For the period on and after January 1, 2012, for covered entities that are not small health plans;

(b) For the period on and after January 1, 2013 for small health plans.

---

## **PART 164—SECURITY AND PRIVACY**

---

### **Contents**

#### Subpart A—General Provisions

§ 164.102 Statutory basis.  
§ 164.103 Definitions.  
§ 164.104 Applicability.  
§ 164.105 Organizational requirements.  
§ 164.106 Relationship to other parts.

#### Subpart B [Reserved]

#### Subpart C—Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability.  
§ 164.304 Definitions.  
§ 164.306 Security standards: General rules.  
§ 164.308 Administrative safeguards.  
§ 164.310 Physical safeguards.  
§ 164.312 Technical safeguards.  
§ 164.314 Organizational requirements.  
§ 164.316 Policies and procedures and documentation requirements.  
§ 164.318 Compliance dates for the initial implementation of the security standards.  
Appendix A to Subpart C of Part 164—Security Standards: Matrix

#### Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information

§ 164.400 Applicability.  
§ 164.402 Definitions.  
§ 164.404 Notification to individuals.  
§ 164.406 Notification to the

media.  
§ 164.408 Notification to the Secretary.  
§ 164.410 Notification by a business associate.  
§ 164.412 Law enforcement delay.  
§ 164.414 Administrative requirements and burden of proof.

#### Subpart E—Privacy of Individually Identifiable Health Information

§ 164.500 Applicability.  
§ 164.501 Definitions.  
§ 164.502 Uses and disclosures of protected health information: general rules.  
§ 164.504 Uses and disclosures: Organizational requirements.  
§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.  
§ 164.508 Uses and disclosures for which an authorization is required.  
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.  
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.  
§ 164.514 Other requirements relating to uses and disclosures of protected health information.  
§ 164.520 Notice of privacy practices for protected health information.  
§ 164.522 Rights to request privacy protection for protected health information.  
§ 164.524 Access of individuals to protected health information.  
§ 164.526 Amendment of protected health information.  
§ 164.528 Accounting of disclosures of protected health information.  
§ 164.530 Administrative requirements.

§ 164.532 Transition provisions.  
§ 164.534 Compliance dates for initial implementation of the privacy standards.

---

AUTHORITY: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

SOURCE: 65 FR 82802, Dec. 28, 2000, unless otherwise noted.

#### **Subpart A—General Provisions**

##### **§ 164.102 Statutory basis.**

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and sections 13400-13424 of Public Law 111-5.

[78 FR 5692, Jan. 25, 2013]

##### **§ 164.103 Definitions.**

As used in this part, the following terms have the following meanings:

*Common control* exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

*Common ownership* exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

*Covered functions* means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

*Health care component* means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).

*Hybrid entity* means a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D).

*Law enforcement official* means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of law; or
- (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

*Plan sponsor* is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

*Required by law* means a mandate contained in law that compels an entity to make a use

or disclosure of protected health information and that is enforceable in a court of law.

*Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009]

#### **§ 164.104 Applicability.**

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

#### **§ 164.105 Organizational requirements.**

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

(A) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(B) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse,” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to “electronic protected health information” refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's

work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

(c)(1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section

for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

**§ 164.106 Relationship to other parts.**

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

**Subpart B [Reserved]**

**Subpart C—Security Standards for the Protection of Electronic Protected Health Information**

AUTHORITY: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.

SOURCE: 68 FR 8376, Feb. 20, 2003, unless otherwise noted.

**§ 164.302 Applicability.**

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

**§ 164.304 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in this subpart, not as used in subparts D or E of this part.)

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

*Authentication* means the corroboration that a person is the one claimed.

*Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control

that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Security or Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

**§ 164.306 Security standards: General rules.**

*(a) General requirements.*

Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

*(b) Flexibility of approach.*

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation

specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications.* In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of

electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

**§ 164.308 Administrative safeguards.**

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision (Addressable).* Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) *Standard: Information access management.* Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions (Required).* If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) *Access authorization (Addressable).* Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right

of access to a workstation, transaction, program, or process.

(5)(i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications.* Implement:

(A) *Security reminders (Addressable).* Periodic security updates.

(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management (Addressable).* Procedures for creating, changing, and safeguarding passwords.

(6)(i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7)(i) *Standard: Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based

initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that



meets the applicable requirements of § 164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.310 Physical safeguards.**

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Facility access controls.* Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

*(2) Implementation specifications:*

(i) *Contingency operations (Addressable).* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan (Addressable).* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures (Addressable).* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to

software programs for testing and revision.

(iv) *Maintenance records (Addressable).* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

*(2) Implementation specifications:*

(i) *Disposal (Required).* Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use (Required).* Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable).* Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable).* Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.312 Technical safeguards.**

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

*(2) Implementation specifications:*

(i) *Unique user identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required)*. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)*. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications*:

(i) *Integrity controls (Addressable)*. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

#### **§ 164.314 Organizational requirements.**

(a)(1) *Standard: Business associate contracts or other arrangements*. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required)*.

(i) *Business associate contracts*. The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) *Other arrangements*. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors*. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) *Standard: Requirements for group health plans*. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected

health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation specifications (Required)*. The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

**§ 164.316 Policies and procedures and documentation requirements.**

A covered entity or business associate must, in accordance with § 164.306:

(a) *Standard: Policies and procedures*. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) *Standard: Documentation*. (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications*:

(i) *Time limit (Required)*. Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required)*. Make documentation available to those persons responsible for implementing the procedures to

which the documentation pertains.

(iii) *Updates (Required)*. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

**§ 164.318 Compliance dates for the initial implementation of the security standards.**

(a) *Health plan*. (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) *Health care clearinghouse*. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) *Health care provider*. A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

**Appendix A to Subpart C of Part  
164—Security Standards: Matrix**

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure (A)
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
<b>Physical Safeguards</b>		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
<b>Technical Safeguards</b> (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)

**Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

**§ 164.400 Applicability.**

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

**§ 164.402 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or

disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

*Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

[78 FR 5695, Jan. 25, 2013]

**§ 164.404 Notification to individuals.**

(a) *Standard* —(1) *General rule.* A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification* —(1) *Elements.* The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the

breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) *Plain language requirement.* The notification required by paragraph (a) of this section shall be written in plain language.

(d) *Implementation specifications: Methods of individual notification.* The notification required by paragraph (a) of this section shall be provided in the following form:

(1) *Written notice.* (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as

specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) *Substitute notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) *Additional notice in urgent situations.* In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

#### **§ 164.406 Notification to the media.**

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

#### **§ 164.408 Notification to the Secretary.**

(a) *Standard.* A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) *Implementation specifications: Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

#### **§ 164.410 Notification by a business associate.**

(a) *Standard* —(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach

is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) *Implementation specifications: Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42740, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

#### **§ 164.412 Law enforcement delay.**

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

#### **§ 164.414 Administrative requirements and burden of proof.**

(a) *Administrative requirements.* A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

#### **Subpart E—Privacy of Individually Identifiable Health Information**

AUTHORITY: 42 U.S.C. 1320d-2, 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279.

#### **§ 164.500 Applicability.**

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of



this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

(d) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5695, Jan. 25, 2013]

#### **§ 164.501 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Correctional institution* means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal

justice system, witnesses, or others awaiting charges or trial.

*Data aggregation* means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

*Designated record set* means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

*Direct treatment relationship* means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

*Health care operations* means any of the following activities of the covered entity to the extent that the

activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud

and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

*Health oversight agency* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from

or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

*Indirect treatment relationship* means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

*Inmate* means a person incarcerated in or otherwise confined to a correctional institution.

*Marketing:* (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is

reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

*Payment* means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

*Psychotherapy notes* means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

*Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

*Public health authority* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

*Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

*Treatment* means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 42769, Aug. 24, 2009; 78 FR 5695, Jan. 25, 2013]

**§ 164.502 Uses and disclosures of protected health information: General rules.**

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i),

pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures.*

(i) *Use and disclosure of genetic information for underwriting purposes:* Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.	(iii) For treatment and payment purposes pursuant to § 164.506(a);	minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.	(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);	(2) <i>Minimum necessary does not apply.</i> This requirement does not apply to:
(ii) <i>Sale of protected health information:</i>	(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;	(i) Disclosures to or requests by a health care provider for treatment;
(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.	(vi) To an individual, when requested under § 164.524 or § 164.528;	(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
(B) For purposes of this paragraph, sale of protected health information means:	(vii) Required by law as permitted under § 164.512(a); and	(iii) Uses or disclosures made pursuant to an authorization under § 164.508;
(1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.	(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.	(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
(2) Sale of protected health information does not include a disclosure of protected health information:		(v) Uses or disclosures that are required by law, as described by § 164.512(a); and
(i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);	(b) <i>Standard: Minimum necessary</i>	(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.
(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;	(1) <i>Minimum necessary applies.</i> When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the	(c) <i>Standard: Uses and disclosures of protected health information subject to an agreed upon restriction.</i> A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).
		(d) <i>Standard: Uses and disclosures of de-identified protected health information.</i>
		(1) <i>Uses and disclosures to create de-identified information.</i> A covered entity may use protected health information to create information that

is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, *i.e.*, de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the

subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

(g)(1) *Standard: Personal representatives.* As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) *Implementation specification: adults and emancipated minors.* If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)(i) *Implementation specification: unemancipated minors.* If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an

individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

(C) Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) *Implementation specification: Deceased individuals.* If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) *Implementation specification: Abuse, neglect, endangerment situations.* Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(h) *Standard: Confidential communications.* A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) *Standard: Uses and disclosures consistent with notice.* A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) *Standard: Disclosures by whistleblowers and workforce member crime victims*

(1) *Disclosures by whistleblowers.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has

engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) *Disclosures by workforce members who are victims of a crime.* A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 78 FR 5696, Jan. 25, 2013]

**§ 164.504 Uses and disclosures: Organizational requirements.**

(a) *Definitions.* As used in this section:

*Plan administration functions* means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

*Summary health information* means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)-(d) [Reserved]

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable

steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.



<p>(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and</p>	<p>business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.</p>	<p>information received by the business associate in its capacity as a business associate to the covered entity, if necessary:</p>
<p>(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.</p>	<p>(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.</p>	<p>(A) For the proper management and administration of the business associate; or</p> <p>(B) To carry out the legal responsibilities of the business associate.</p> <p>(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:</p> <p>(A) The disclosure is required by law; or</p>
<p>(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.</p>	<p>(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.</p>	<p>(B)(I) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and</p>
<p>(3) <i>Implementation specifications: Other arrangements.</i> (i) If a covered entity and its business associate are both governmental entities:</p>	<p>(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.</p>	<p>(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.</p>
<p>(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.</p>	<p>(4) <i>Implementation specifications: Other requirements for contracts and other arrangements.</i> (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health</p>	<p>(5) <i>Implementation specifications: Business associate contracts with subcontractors.</i> The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.</p>
<p>(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the</p>		

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such

information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and

(iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) *Standard: Requirements for a covered entity with multiple covered functions.*

(1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation

specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5697, Jan. 25, 2013]

**§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.**

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.*

(1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is

required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.* (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5698, Jan. 25, 2013]

**§ 164.508 Uses and disclosures for which an authorization is required.**

(a) *Standard: Authorizations for uses and disclosures* —(1) *Authorization required: General rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: Psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a);

§ 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) *Authorization required: Sale of protected health information.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) *Implementation specifications: General requirements*

(1) *Valid authorizations.*

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) *Defective authorizations.* An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an

authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) *Prohibition on conditioning of authorizations.* A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) *Revocation of authorizations.* An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) *Documentation.* A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) *Implementation specifications: Core elements and requirements*

(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including

for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) *Required statements.* In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health

plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5699, Jan. 25, 2013]

**§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.**

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) *Standard: Use and disclosure for facility directories*

(1) *Permitted uses and disclosure.* Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Use or disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) *Opportunity to object.* A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) *Emergency circumstances.* (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) *Standard: Uses and disclosures for involvement in the individual's care and notification purposes*

(1) *Permitted uses and disclosures.*

(i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

(2) *Uses and disclosures with the individual present.* If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) *Limited uses and disclosures when the individual is not present.* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health

information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013]

**§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.**

A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure

permitted by this section, the covered entity's information and the individual's agreement may be given orally.

(a) *Standard: Uses and disclosures required by law.*

(1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) *Standard: Uses and disclosures for public health activities.* (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity

for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:



(1) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

(2) *Permitted uses.* If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) *Standard: Disclosures about victims of abuse, neglect or domestic violence*

(1) *Permitted disclosures.* Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the

individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) *Informing the individual.* A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(d) *Standard: Uses and disclosures for health oversight activities*

(1) *Permitted disclosures.* A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal

proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) *Exception to health oversight activities.* For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) *Joint activities or investigations.* Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) <i>Permitted uses.</i> If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.	assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:	(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
(e) <i>Standard: Disclosures for judicial and administrative proceedings</i>	(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);	(v) For purposes of paragraph (e)(1) of this section, a <i>qualified protective order</i> means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
(1) <i>Permitted disclosures.</i> A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:	(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and	(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or	(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:	(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.
(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:	(1) No objections were filed; or	(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.
(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or	(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.	
(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.	(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:	(2) <i>Other uses and disclosures under this section.</i> The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.
(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory	(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or	

(f) *Standard: Disclosures for law enforcement purposes.* A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) *Permitted disclosures: Pursuant to process and as otherwise required by law.* A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

(2) *Permitted disclosures: Limited information for identification and location purposes.* Except for

disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) *Permitted disclosure: Victims of a crime.* Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a

law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) *Permitted disclosure: Decedents.* A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) *Permitted disclosure: Crime on premises.* A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith

constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

*(6) Permitted disclosure: Reporting crime in emergencies.*

(i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

*(g) Standard: Uses and disclosures about decedents.*

(1) *Coroners and medical examiners.* A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health

information for the purposes described in this paragraph.

(2) *Funeral directors.* A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) *Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes.* A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

*(i) Standard: Uses and disclosures for research purposes*

(1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34

CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) *Reviews preparatory to research.* The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) *Research on decedent's information.* The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and	oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;	(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;
(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.	(B) The research could not practicably be conducted without the waiver or alteration; and	
(2) <i>Documentation of waiver approval.</i> For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:	(C) The research could not practicably be conducted without access to and use of the protected health information.	
(i) <i>Identification and date of action.</i> A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;	(iii) <i>Protected health information needed.</i> A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;	(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and
(ii) <i>Waiver criteria.</i> A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:	(iv) <i>Review and approval procedures.</i> A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:	
(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;	(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);	(v) <i>Required signature.</i> The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.
(1) An adequate plan to protect the identifiers from improper use and disclosure;		(j) <i>Standard: Uses and disclosures to avert a serious threat to health or safety</i>
(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and		(1) <i>Permitted disclosures.</i> A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:
(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized		(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) *Use or disclosure not permitted.* A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) *Limit on information that may be disclosed.* A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) *Presumption of good faith belief.*

A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) *Standard: Uses and disclosures for specialized government functions.*

(1) *Military and veterans activities*

(i) *Armed Forces personnel.* A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

(iii) *Veterans.* A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) *Foreign military personnel.* A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.

(2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.*, Executive Order 12333).

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) *Medical suitability determinations.* A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual

was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

- (i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;
- (ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or
- (iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) *Correctional institutions and other law enforcement custodial situations.*

(i) *Permitted disclosures.* A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) *Permitted uses.* A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) *No application after release.* For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) *Covered entities that are government programs providing public benefits.*

(i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered

functions of such programs or to improve administration and management relating to the covered functions of such programs.

(l) *Standard: Disclosures for workers' compensation.* A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

#### **§ 164.514 Other requirements relating to uses and disclosures of protected health information.**

(a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with

other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and	(G) Social security numbers;	is not otherwise capable of being translated so as to identify the individual; and
(ii) Documents the methods and results of the analysis that justify such determination; or	(H) Medical record numbers;	
	(I) Health plan beneficiary numbers;	(2) <i>Security</i> . The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.
(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:	(J) Account numbers;	
	(K) Certificate/license numbers;	
	(L) Vehicle identifiers and serial numbers, including license plate numbers;	(d)(1) <i>Standard: Minimum necessary requirements</i> . In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.
(A) Names;	(M) Device identifiers and serial numbers;	
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:	(N) Web Universal Resource Locators (URLs);	(2) <i>Implementation specifications: Minimum necessary uses of protected health information</i> .
(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and	(O) Internet Protocol (IP) address numbers;	(i) A covered entity must identify:
(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.	(P) Biometric identifiers, including finger and voice prints;	(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;	(Q) Full face photographic images and any comparable images; and	(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.
	(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and	(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.
(D) Telephone numbers;	(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.	
(E) Fax numbers;	(c) <i>Implementation specifications: Re-identification</i> . A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:	(3) <i>Implementation specification: Minimum necessary disclosures of protected health information</i> .
(F) Electronic mail addresses;	(1) <i>Derivation</i> . The code or other means of record identification is not derived from or related to information about the individual and	(i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must



implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) *Implementation specifications: Minimum necessary requests for protected health information.*

(i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) *Implementation specification: Other content requirement.* For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) *Standard: Limited data set.* A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2)

and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) *Implementation specification: Limited data set:* A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.	(B) Establish who is permitted to use or receive the limited data set; and	(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.
(3) <i>Implementation specification: Permitted purposes for uses and disclosures.</i>	(C) Provide that the limited data set recipient will:	(f) <i>Fundraising communications.</i>
(i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.	(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;	(1) <i>Standard: Uses and disclosures for fundraising.</i> Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:
(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.	(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;	(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;
(4) <i>Implementation specifications: Data use agreement</i>	(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;	(ii) Dates of health care provided to an individual;
(i) <i>Agreement required.</i> A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.	(4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and	(iii) Department of service information;
(ii) <i>Contents.</i> A data use agreement between the covered entity and the limited data set recipient must:	(5) Not identify the information or contact the individuals.	(iv) Treating physician;
(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;	(iii) <i>Compliance.</i>	(v) Outcome information; and
	(A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:	(vi) Health insurance status.
	(1) Discontinued disclosure of protected health information to the recipient; and	(2) <i>Implementation specifications: Fundraising requirements.</i> (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.
	(2) Reported the problem to the Secretary.	(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the

individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) *Standard: Verification requirements.* Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) *Implementation specifications: Verification.*

(i) *Conditions on disclosures.* If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) *Identity of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health

information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) *Authority of public officials.* A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) *Exercise of professional judgment.* The verification requirements of this paragraph are

met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013]

**§ 164.520 Notice of privacy practices for protected health information.**

*(a) Standard: notice of privacy practices,*

(1) *Right to notice.* Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) *Exception for group health plans.*

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary

health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(3) *Exception for inmates.* An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

*(b) Implementation specifications: Content of notice.*

(1) *Required elements.* The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) *Header.* The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED

AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

(ii) *Uses and disclosures.* The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications;

(B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan*, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) *Individual rights.* The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) *Covered entity's duties.* The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to

make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) *Complaints.* The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) *Contact.* The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) *Effective date.* The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

## (2) *Optional elements.*

(i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii),

the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) *Revisions to the notice.* The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) *Implementation specifications: Provision of notice.* A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) *Specific requirements for health plans.*

(i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) *Specific requirements for certain covered health care providers.* A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) *Specific requirements for electronic notice.*

(i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided

to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) *Implementation specifications: Joint notice by separate covered entities.* Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(e) *Implementation specifications: Documentation.* A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

#### **§ 164.522 Rights to request privacy protection for protected health information.**

(a)(1) *Standard: Right of an individual to request restriction of uses and disclosures.*

(i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

(vi) A covered entity must agree to the request of an individual to restrict

disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

(b)(1) *Standard: Confidential communications requirements.*

(i) A covered health care provider must permit individuals to request

and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) *Implementation specifications: Conditions on providing confidential communications.*

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

**§ 164.524 Access of individuals to protected health information.**

(a) *Standard: Access to protected health information.*

(1) *Right of access.* Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(2) *Unreviewable grounds for denial.* A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.



(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by

paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) *Review of a denial of access.* If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) *Implementation specifications: Requests for access and timely action.*

(1) *Individual's request for access.* The covered entity must permit an individual to request access to inspect or to obtain a copy of the

protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) *Timely action by the covered entity.* (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) *Implementation specifications: Provision of access.* If the covered entity provides an individual with

access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Providing the access requested.* The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) *Form of access requested.*

(i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access

to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) *Fees.* If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) *Implementation specifications: Denial of access.* If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) *Making other information accessible.* The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) *Denial.* The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) *Other responsibility.* If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) *Review of denial requested.* If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

[65 FR 82823, Dec. 28, 2000, as amended at 78 FR 5701, Jan. 25, 2013]

**§ 164.526 Amendment of protected health information.**

(a) *Standard: Right to amend.* (1) *Right to amend.* An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) *Denial of amendment.* A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) *Implementation specifications: Requests for amendment and timely action.*

(1) *Individual's request for amendment.* The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record

set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) *Timely action by the covered entity.*

(i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) *Implementation specifications: Accepting the amendment.* If the covered entity accepts the requested amendment, in whole or in part, the

covered entity must comply with the following requirements.

(1) *Making the amendment.* The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) *Informing the individual.* In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) *Informing others.* The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) *Implementation specifications: Denying the amendment.* If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) *Denial.* The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) *Statement of disagreement.* The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) *Rebuttal statement.* The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered

entity must provide a copy to the individual who submitted the statement of disagreement.

(4) *Recordkeeping.* The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) *Future disclosures.* (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) *Implementation specification: Actions on notices of amendment.* A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) *Implementation specification: Documentation.* A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

**§ 164.528 Accounting of disclosures of protected health information.**

(a) *Standard: Right to an accounting of disclosures of protected health information.* (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- (i) To carry out treatment, payment and health care operations as provided in § 164.506;
- (ii) To individuals of protected health information about them as provided in § 164.502;
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
- (iv) Pursuant to an authorization as provided in § 164.508;
- (v) For the facility's directory or to persons involved in the individual's

care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) *Implementation specifications: Content of the accounting.* The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the

same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to

whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) *Implementation specifications: Provision of the accounting.* (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) *Implementation specification: Documentation.* A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

#### **§ 164.530 Administrative requirements.**

(a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) *Implementation specification: Personnel designations.* A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.* (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in

paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) *Implementation specification: Safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) *Standard: Complaints to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) *Implementation specification: Documentation of complaints.* As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) *Standard: Sanctions.* A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the

covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) *Implementation specification: Documentation.* As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) *Standard: Mitigation.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) *Standard: Refraining from intimidating or retaliatory acts.* A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in § 160.316 of this subchapter.

(h) *Standard: Waiver of rights.* A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) *Standard: Policies and procedures.* A covered entity must implement policies and procedures

with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) *Standard: Changes to policies and procedures.* (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) *Implementation specification: Changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's

policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) *Implementation specifications: Changes to privacy practices stated in the notice.* (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) *Implementation specification: Changes to other policies or procedures.* A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) *Standard: Documentation.* A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation



required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) *Standard: Group health plans.* (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 71 FR 8433, Feb. 16, 2006; 74 FR 42769, Aug. 24, 2009]

#### § 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained

from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).

(b) *Implementation specification: Effect of prior authorization for purposes other than research.* Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) *Implementation specification: Effect of prior permission for research.* Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) *Covered entity responsibilities.* Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) *Effect of prior data use agreements.* If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 78 FR 5702, Jan. 25, 2013]

**§ 164.534 Compliance dates for initial implementation of the privacy standards.**

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) *Health plans other than small health plans.* April 14, 2003.

(2) *Small health plans.* April 14, 2004.

(c) *Health clearinghouses.* A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

# GDPR CONSULTING SERVICES FOR INVESTMENT FIRMS

**The European Union's General Data Protection Regulation (GDPR) comes into effect on the 25th of May 2018. It will have a significant impact on any organization servicing European Resident data, irrespective of where that institution is based.**

## MARKET VIEW

The responsibilities facing firms are both broad and onerous, with GDPR spanning 99 Articles and 173 Recitals. The penalties for getting it wrong are severe. Depending on the scale of the breach, non-compliance can lead to fines of up to €20 million EUR or 4% of annual turnover (whichever is greater).

Any firm that processes data related to EU residents – need to take action to mitigate the risks of non-compliance.

## SOLUTION

Cordium offers GDPR compliance consultation services that combine our cyber and information security expertise to assist firms with selecting the appropriate GDPR Compliance and Data Privacy Management Platform.

### ANALYSIS OF POLICIES AND PROCEDURES

The analysis will cover a full range of obligations, including the basis for collecting and processing data, the rights of data subjects, specific obligations of data controllers and processors, privacy notifications, information security, incident management processes, privacy by design, data protection and data transfer mechanisms.

### REMEDATION PLANNING, IMPLEMENTATION AND ONGOING SUPPORT

Based on weaknesses and gaps in policies, procedures and data processes identified from our initial analysis, Cordium can devise and, in conjunction with you, implement a remediation plan specific to each firm's requirements. We provide a controls audit, ensuring private data has been secured effectively, and that remediation efforts have not only succeeded in meeting GDPR compliance requirements but also addressed any potential vulnerability in a firm's data security architecture.

### INFORMATION AND DATA PROCESSING SECURITY REVIEW

Our team of experts will work with you to map out the existing workflows relating to the collection, processing and storage of the EU Resident data. They can assist with establish records of all data processing activities relevant to GDPR. This includes vendor third party risk management with regard to their handling of your EU Resident data.

In addition, our experts can review your security control implementations, including encryption of data both in-transit and at-rest, user authentication and privileged access controls, incident response protocols and data sovereignty obligations with regards to the physical location where data is stored. And they can assist with the development or refinement of your company's incident response policies and procedures to ensure they are compliant with GDPR requirements, should a data privacy compromise occur.



New York  
Boston  
San Francisco  
London  
Malta  
Hong Kong

[cordium.com](http://cordium.com)



## GDPR CONSULTING SERVICES FOR INVESTMENT FIRMS

### BENEFITS

#### DEEP INDUSTRY KNOW-HOW

Cordium's team offers deep domain expertise to interpret the specific impact to investment firms and understands the requirements of each line of business and can interpret how GDPR fits with existing compliance obligations.

#### PROVEN SOLUTIONS

Firms looking to comply with GDPR need to act quickly. Cordium leverages proven methodologies to identify potential compliance gaps and quickly embark on a remediation program to close those gaps. In addition, we work with leading third party solution providers to ensure you have the right tools and technologies to support compliance.

#### TECHNICAL EXPERTISE

Our consultants do more than approach GDPR as a box ticking exercise. We draw on our information and cyber security expertise to ensure you have the right policies, processes, controls, and infrastructure to secure your private data at all times. Whether it relates to vendor management, data encryption, user authentication or privileged access controls, we ensure you maintain a tight handle on any potential vulnerabilities.

New York  
Boston  
San Francisco  
London  
Malta  
Hong Kong

**cordium.com**

---

### ABOUT CORDIUM

Cordium is a market-leading provider of governance, risk and compliance services to the asset management and securities industry. Cordium has offices in London, New York, Boston, San Francisco, Malta and Hong Kong. The firm employs more than 200 experienced professionals who support over 1,500 clients in the financial services industry.

# International Cybersecurity Compliance Concerns

By Steven Rubin and  
Stephen Milne

Compared with the rest of the world, the United States has historically been a more open framework when dealing with information. Social media has made even the most mundane and possibly personal pieces of data available to many with a press of a finger. Such an open relinquishment of private information is almost assumed, and has become part of the American culture. Those who think about how easy it is to access data understand how their own data has become part of the searchable cyberspace.

The European culture and laws are different. Privacy rights are assumed, information confidentiality is maintained, and the concept of the United States “discovery” is scorned. There is a concern that European sensitive data should stay outside of the United States due to the protection of such data in the country not being sufficiently

strong. It is therefore not a surprise that the laws in the United States and in Europe are inconsistent when it comes to cybersecurity.

## CYBERSECURITY LAW IN THE UNITED STATES

The most significant piece of federal legislation in this area is the Cybersecurity Information Sharing Act (CISA), passed in December 2015. The purpose of this Act, purportedly, is to promote information sharing between the government and the private sector for issues relating to cybersecurity and new threat vectors. The idea is that sometimes industry is aware of new viruses or technical threats, but does not share the information with the government so that the government may protect itself and/or inform the public. CISA creates a voluntary means for companies to share their threat data with the government.

There are problems with sharing this information. While the act of sharing appears to be protected by statute, the underlying problem may not be. If I see a threat to my system, I could tell the government about that threat, and the act of telling would not create a new cause of action. But the law is not clear

as to whether that sharing could then lead to a lawsuit relating to the *cause* of the sharing. Stated another way, I can tell the government I have a virus, and telling the government should not itself expose my company to liability. But I could later get sued for failing to comply with certain cybersecurity requirements because my system was infected with a virus and I did not take proper steps to protect the data.

So, trying to comply with United States laws alone creates a dilemma. But if you consider complying with CISA, you may also expose yourself to legal issues in Europe.

## EUROPEAN LAWS ON CYBERSECURITY

Disclosure of personal data (capable of being used to identify a living person either on its own, or in conjunction with other data in the possession of the person controlling how the data is used) that relates to EU nationals could cause serious potential issues in light of recent developments overseas. Previously (before January 2016), many organizations relied upon the approved “Safe Harbor” regime framework developed by the Department of Commerce (DOC) in

---

**Steven Rubin** is a partner with Moritt Hock & Hamroff LLP in New York. **Stephen Milne** is a consultant with Memery Crystal LLP in London.



the United States and the European Commission, under which organizations could self-certify that they adhered to its principles. The certifying company gave binding promises that they complied with privacy policy requirements and provided protections for personal data which were sufficiently high that transfers of personal data from the EU to the United States would be permissible under the applicable Data Protection Directive (the Directive).

However, the Safe Harbor regime has suffered a huge blow by virtue of a recent decision in the Court of Justice of the European Union (CJEU). Maximillian Schrems was an Austrian citizen who had been a Facebook user since 2008. Facebook habitually transferred some data provided by its EU-based subscribers from its Irish subsidiary to servers located in the United States. Mr. Schrems lodged a complaint with the relevant supervisory authority in Ireland on the basis that the law and practice in the United States did not provide sufficient protection in relation to his data.

Initially, Mr. Schrems' complaint was rejected, particularly on the basis that the Safe Harbor regime ensured sufficient protection. However, on referral to the CJEU, the court held that the powers available to national supervisory authorities cannot be eliminated just because the European Commission originally decided that the Safe Harbor scheme provided such protection. The authority must look at the situation independently and determine whether the transfer of a person's data to a third country complies with the requirements of the Directive.

The CJEU then proceeded to consider the fact that public authorities in the United States are not subject to the Safe Harbor scheme. Further, national security, law enforcement and public interest all may prevail to the extent that a United States entity holding or processing data may be forced to ignore the requirements of the Safe Harbor scheme where it conflicts with any of the foregoing. As a result, data would not be protected in such circumstances and there were no clear limitations or restrictions on the public authorities' abilities.

In addition, there was no clear ability for individuals to pursue legal remedies in order to access their data or to have it rectified or erased, which the CJEU viewed as inherent in the existence of the rule of law and as compromising "the essence of the fundamental right to effective judicial protection." The CJEU therefore held that the original European Commission decision that Safe Harbor privacy principles provided adequate protection was invalid — effectively nullifying the Safe Harbor option.

### WHAT NOW?

The Safe Harbor route is no longer a valid basis upon which personal data can be transferred from the European Union to the United States. But there is not, as of yet, clear guidance as to what will replace it. Indeed, different data protection authorities (DPAs) have been taking different approaches to this evolving situation.

For example, the Information Commissioner's Office (ICO; the supervisory data protection authority

for the United Kingdom) has been advocating that continued use of the Safe Harbor principles may still be a sensible proposition in the interim. The ICO further indicated it will not take enforcement procedures yet, until an approved alternative to Safe Harbor has been determined. However, this guidance is not legally binding and the ICO is posed to reiterate that companies need to review their compliance processes and procedures.

This approach has been somewhat reflected in guidance from the Spanish regulator, which has indicated that it will not rush to take enforcement action against companies provided they are working on appropriate proposals and arrangements to ensure adequate protection of personal data. However, in stark contrast, the data protection authority in Hamburg, Germany, has already made it public that it does not expect organizations to continue relying upon Safe Harbor and that it will take immediate enforcement proceedings against any that do continue to transfer personal data outside the EU in this way. Such proceedings could lead to fines up to €300,000 (roughly \$340,000) per data breach.

### SOME PROPOSED EUROPEAN SOLUTIONS

The Article 29 Working Party (which is made up of representatives from the data protection authorities of the EU states) recently confirmed that it views use of binding corporate rules and model contract clauses as valid options to enable the transfer of data from the EU to the United States.

Binding Corporate Rules are essentially rules operated by an organization that put in place adequate safeguards for protecting personal data in line with the Article 29 Working Party's requirements. They are not, however, a quick fix — as such rules require an application to, and approval from, the relevant data protection authority via a relatively cumbersome design and implementation procedure that usually takes in the region of 12-18 months.

Model contract clauses are, on the other hand, considerably easier to implement provided both parties are in agreement. These provide for an approved set of contractual obligations that eliminate the requirement for the transferee of data to make their own assessment regarding the adequacy of the protections provided. There are different sets of clauses depending upon the parties' relationship and what they do with the data.

A further possibility is to obtain express consent to the transfer of the data. However, even the more relaxed data protection authorities are closely scrutinizing this route to effecting transfers, as the key concern is whether consent is specific enough for what is happening to the data and whether it provides any real protection to the individual. Much has been made in recent months of high-profile examples of data having been harvested from individuals on the back of a generic data consent, and having then been retransferred, reused and resold multiple times in manners the individual who gave "consent" could not possibly have anticipated. Consent on its own may well not be enough.

## PRIVACY SHIELD

The European Commission and the DOC have agreed upon a new arrangement, known as the "Privacy Shield," as a replacement for the now defunct Safe Harbor scheme. The Privacy Shield is in fact a collection of principles, including:

**1. Choice** — individuals will have the ability to opt-in or out as far as sensitive data is concerned, as regards third-party marketing and in relation to any new use of their data that was not initially contemplated.

**2. Notice** — individuals must be informed of their rights, the principles of Privacy Shield and given a contact for complaints. They must also be given details of sharing and disclosure of their data (including public authorities), and organizations will have to confirm their liability for data processing.

**3. Accountability** — organizations will be required to put in place formal contract arrangements in writing for onward transfers of data to other controllers or processors (with only limited exceptions).

**4. Security** — security measures must be implemented that are reasonable based on the nature of the processing and the personal data being processed.

**5. Integrity and Limitation** — data will have to be kept up to date and accurate, and data collection will have to be limited strictly to what is relevant in the circumstances.

**6. Access** — individuals will have the right to access their data and to require its correction and/or deletion (unless the cost of doing so would be overly burdensome).

**7. Recourse/enforcement** — this is one of the crucial proposals. It provides for a free means of recourse for individuals to be provided by the organization with the ability for individuals to escalate complaints to local data protection authorities if the issue is not satisfactorily dealt with. If that does not resolve the matter, then there is even scope for individuals to potentially initiate arbitration claims.

Privacy Shield is still a little way off, however, as intended implementation was set for June 2016, but there are still a number of criticisms leveled at it by both politicians and commentators and implementation has been delayed. In addition, the General Data Protection Regulations are upcoming (albeit not until April 2018) and these will bolster both the EU's data protection authorities' powers and their likelihood to crack down on enforcement.

## CONCLUSION

Each organization needs to review its current compliance arrangements and re-evaluate on the basis of the above issues, implementing sensible interim solutions, at least, to avoid falling foul of the more aggressive data protection authorities and their willingness to impose potentially sizeable fines.



# Meeting Your Cybersecurity Obligations

By Steve Rubin and A. Jonathan Trafimow

The Federal Trade Commission ("FTC"), currently the predominate enforcer of cybersecurity regulations, has commented that "security is an ongoing process of using reasonable and appropriate measures in light of the circumstances"<sup>1</sup> which is not covered by any checklist.<sup>2</sup> Failure to take appropriate steps to adequately come into compliance subjects a business to possible enforcement actions by agencies, lawsuits from affected consumers and fines from various state regulations. Compliance with the number and complexity of federal and state cybersecurity laws and regulations is no simple task. In this evolving legal environment, a Written Information Security Plan ("WISP") provides the necessary structure companies need to identify and implement conforming practices. A WISP not only allows a company to adapt to industry and regulatory changes, but also incorporates legal principles to mitigate damages in the event of an incident.

## Cybersecurity Regulations—Specific and General

Nearly every business is subject to some form of cyber security regulation. The U.S. Securities and Exchange Commission (the "SEC"), Office of the Comptroller of the Currency (the "OCC"), and Centers for Medicare & Medicaid Services (the "CMS"), along with several other state and federal agencies, have all begun to incorporate cybersecurity principles into their regulations. This has led to a myriad of rules, each having its own jurisdictional scope and requirements. These rules generally require a number of technical safeguards, such as the implementation of firewalls, anti-virus software, system audits and that the company's security standards be documented. But, depending on the type of information a business collects, agencies may also impose additional constraints. Where information has traditionally been highly regulated, agencies have begun to require specific safeguards. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that covered entities restrict and document access to protected health information;<sup>3</sup> determine which applications are important to patient care;<sup>4</sup> and record the movement of hardware and electronic media.<sup>5</sup> For registered investment companies and advisors, the SEC has provided that failure to prepare for a cyber incident could result in a breach of their fiduciary obligations,<sup>6</sup> and make the company liable for fraudulent activity.<sup>7</sup> The SEC has also suggested that a covered entity's cybersecurity obligations may extend to commercial or market-sensitive information.<sup>8</sup> Finally, the Sarbanes-Oxley Act of 2002 ("SOX") imposes severe penalties on corporate officials who fail to implement internal controls, including technical safeguards,<sup>9</sup> to ensure the truth and accuracy of each annual or quarterly report.<sup>10</sup>

Even when a company's practices are not regulated by the above agencies, they may still be subject to the regulations of the FTC. Under section 5(a) of the Federal Trade Commission Act ("FTCA"), the FTC may sue any business subject to its jurisdiction for engaging in "acts or practices in or affecting commerce" that are "unfair" or "deceptive."<sup>11</sup> The FTC has brought several actions against defendants where those defendants claimed to have reasonable security, but failed to implement sufficient measures to prevent, detect, and respond to unauthorized access to their computer networks.<sup>12</sup> As a result, companies have been subjected to fines, required to implement a comprehensive information security plan and obligated to obtain audits by independent third party security professionals for 20 years.

A company's compliance obligations do not stop with its internal practices, but also extend to their relations with company affiliates. In *GMR Transcription Services, Inc.*, the FTC found that the defendant failed to implement reasonable and appropriate security by not contractually requiring appropriate safeguards and not monitoring its vendor to ensure its compliance.<sup>13</sup> While a company may not be able to directly control its affiliates' practices, a business can nonetheless take precautions to show that it assessed its affiliates' cybersecurity and required them to implement appropriate safeguards.

As a part of any information security program, counsel should review any vendor agreements along with its vendor's WISPs and security audits. Attorneys should make sure that these agreements include, among other things, a provision mandating notification if the vendor updates its security practices or significantly changes its operating procedures. While it is unclear what constitutes appropriate monitoring, counsel should review its vendors' WISPs to assess their cybersecurity practices. Depending on the nature of the information being shared, it may be necessary to require the vendor to undergo a security audit immediately or at random intervals throughout the business relationship.

A company's cybersecurity practices need not be perfect. Where a company has taken every reasonable precaution, the FTC has provided that a breach "will not violate the laws that [it] enforces."<sup>14</sup> Companies seeking to implement appropriate cybersecurity safeguards should ensure their WISP is in compliance with the National Institute of Standards and Technology's Cybersecurity Framework ("NIST Framework"). In response to growing cybersecurity concerns, President Obama signed Executive Order 13636 which directed the National Institute of Standards and Technology to develop a Cybersecurity Framework. Following the release of the draft standards, on February 12, 2014, the final NIST Framework took effect. The FTC



has already stated that the NIST Framework “is fully consistent with the FTC’s enforcement framework”<sup>15</sup> as to matters of risk assessment and mitigation.

### WISP Comes to the Rescue

As an essential part of a cybersecurity program and before a potential breach occurs, companies need to develop a WISP, an internal company document that enumerates a company’s regulatory requirements, risks and responses to determine its conformity. A WISP identifies and ranks the critical components of a business according to its business objectives and legal obligations. The company can then concentrate its available resources in areas requiring heightened security and eliminate those where such protection is not incumbent. As a company’s obligations fluctuate, a WISP offers an effective means of continuing to provide appropriate safeguards.

As a result of technological developments and changes in business practices, companies must continuously adapt their security structure to meet the demands of new regulations and industry best practices. Events such as acquiring business from other countries, outsourcing company functions and utilizing new software can all have profound effects on a business’s compliance needs. A WISP pinpoints how data traverses a company’s network and helps identify gaps in its security practices. A company can then assess potential risks and implement reasonable cost-effective responses to meet its regulatory requirements.

While the law continues to struggle to keep up with technology, old regulations may be interpreted broadly in an attempt to address the technologically changing landscape. A WISP structures a company’s review and organization of its cybersecurity infrastructure and facilitates improvements. For example, a WISP can develop a record of how a company: identifies sensitive information, addresses threats, manages risk and continuously improves its security infrastructure by learning from previous incidents. Without such a structure, a business may fail to recognize a critical component of its cybersecurity framework and will be less prepared to adapt to the evolving law.

### A WISP Can Limit Customer Actions

The benefits of a WISP are not limited to proving a company’s regulatory compliance; it also has the potential to limit customer lawsuits by showing a company took reasonable steps to protect its data. As discussed below, companies that can demonstrate that their stolen data was effectively protected or that they employed reasonable practices but could not prevent an incident (both of which are required in a WISP), may persuade a court to dismiss an action. In one case, several tapes containing protected information, including medical records and social security numbers, were stolen.<sup>16</sup> Yet, the court

determined that the plaintiffs had not suffered an injury-in-fact because defendant’s practice of storing encrypted data on tapes made it unlikely the attacker would be able to “open and decipher” the stolen information.<sup>17</sup> In another case, the court found that even though unencrypted customer data was stolen, the company had not violated its duty of reasonable care.<sup>18</sup> The court reasoned the event was unforeseeable, and that defendant acted reasonably by “transmitt[ing] and us[ing] data in accordance” with its WISP.<sup>19</sup>

### Lawyers Provide Even More Protection by Protecting Your WISP

Legal counsel is an integral part of the WISP creation process because the utilization of legal advice in connection with the WISP creates an argument that at least some aspects of the process are shielded from disclosure in litigation because of the attorney-client privilege or attorney work product doctrine. Where a lawyer needs outside help to provide effective consultation to the lawyer’s client, the attorney-client privilege may attach.<sup>20</sup> To be covered by the doctrine, a document must have “been prepared in anticipation of litigation by or for a party, or by the party’s representative.”<sup>21</sup> The doctrine protects an attorney’s mental impressions, which receive virtually unlimited protection, and work product.<sup>22</sup> Both the attorney-client privilege and attorney work product can be waived.<sup>23</sup> As constructing a WISP requires a thorough review of a company’s procedures and technical practices, counsel should take every precaution to preserve a company’s potential claims of privilege and work product.

### Conclusion

While technology continues to evolve, so will the complexities of a company’s cybersecurity obligations. It will not be long before all companies are subjected to at least some form of cybersecurity compliance. Having a properly drafted WISP can help your business comply with this ever-changing legal environment.

### Endnotes

1. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation’s Cyberspace*, FED. TRADE COMM’N (Apr. 21, 2004) (statement of Orson Swindle, Former Commissioner, FTC), <https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations>.
2. Joseph J. Lazzarotti, *Checklists Not Enough When Developing a WISP*, FTC Director Comments at IAPP Global Privacy Summit, NAT’L L. REV. (Mar. 9, 2015), <http://www.natlawreview.com/article/checklists-not-enough-when-developing-wisp-ftc-director-comments-iapp-global-privacy>.
3. 45 C.F.R. § 164.308(a)(4)(ii)(A) (2013); 45 C.F.R. § 164.308(a)(4)(ii)(C).
4. *Id.* § 164.308(a)(7)(ii)(E).
5. *Id.* § 164.310(d)(2)(iii).

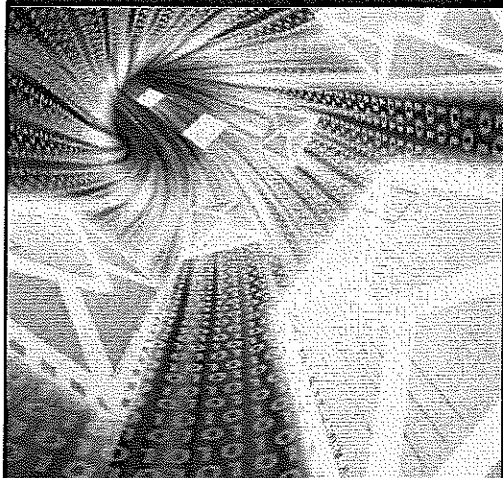
6. See, e.g., 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
7. See, e.g., 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
8. SEC, IM GUIDANCE UPDATE NO. 2015-02 2 (2015), <http://www.sec.gov/investment/im-guidance-2015-02.pdf>.
9. Auditing Standard No. 5, PUB. CO. ACCOUNTING OVERSIGHT BD. (2007), [http://pcaobus.org/Standards/Auditing/Pages/Auditing\\_Standard\\_5.aspx](http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx) (Under section 36 audits include a review of the "effect of information technology on internal controls over financial reporting.").
10. 15 U.S.C. § 7241 (2002).
11. *Id.* § 45(a)(1).
12. *Cord Blood Bank Settles FTC Charges That It Failed to Protect Consumers Sensitive Personal Information*, FED. TRADE COMM'N (Jan. 28, 2013), <http://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers>; *BJ's Wholesale Club Settles FTC Charges*, FED. TRADE COMM'N (June 16, 2005), <http://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges>.
13. *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, FED. TRADE COMM'N (Jan. 31, 2014), <https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>.
14. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation's Cyberspace*, FED. TRADE COMM'N (Apr. 21, 2004), <https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations> ("Although a breach may indicate a problem with a company's security, breaches can happen...even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces.").
15. FED. TRADE COMM'N, *ON THE FRONT LINES: THE FTC'S ROLE IN DATA SECURITY* (2004), [http://www.ftc.gov/system/files/documents/public\\_statements/582841/140917csisspeech.pdf](http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf).
16. *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014).
17. *Id.* at 29.
18. *Guin v. Brazos Higher Educ. Serv. Corp.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483, (D. Minn. Feb. 7, 2006).
19. *Id.*
20. *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961) ("What is vital to the privilege is that the communication be made in confidence for the purpose of obtaining legal advice from the lawyer.").
21. *United States v. Ghavami*, 882 F. Supp. 2d 532, 539 (S.D.N.Y. 2012) (internal citations omitted) (The work product doctrine, partially codified by Rule 26(b)(3) of the Federal Rules of Civil Procedure, is designed to allow "a lawyer [to privately] prepare and develop legal theories and strategy 'with an eye toward litigation.'"); see also *Doe v. Poe*, 244 A.D.2d 450, 451-52 (N.Y. App. Div. 1997), *aff'd*, 92 N.Y.2d 864 (N.Y. App. Div. 1998); *Bras v. Atlas Constr. Corp.*, 153 A.D.2d 914, 915-16 (N.Y. App. Div. 1989).
22. *Ghavami*, 882 F. Supp. 2d at 540.
23. *Id.* (internal citations omitted).

Steven S. Rubin is a partner at Moritt Hock & Hamroff LLP where he chairs the firm's patent practice and co-chairs the firm's cybersecurity practice. With an electrical engineering background, Mr. Rubin concentrates his practice on all phases of patent-related matters, both domestically and internationally.

A. Jonathan Trafimow is a partner at Moritt Hock & Hamroff LLP where he chairs the firm's employment practice and co-chairs the firm's cybersecurity practice. Mr. Trafimow represents employers in all areas of workplace discrimination, retaliation, harassment and civil rights claims, and class actions. He also routinely advises employers on compliance with local and federal employment laws and regulations.

The authors thank Stephen E. Breidenbach, student of the Maurice A. Deane School of Law at Hofstra University, for his assistance in the research and drafting of this article.

## Request for Articles



If you have written an article and would like to have it considered for publication in *Inside*, please send it to either of its editors:

Jessica D. Thaler  
410 Benedict Ave.  
Tarrytown, NY 10591  
[jthaleresq@gmail.com](mailto:jthaleresq@gmail.com)

Elizabeth J. Champnoi  
Stout Risius Ross, Inc. (SRR)  
120 West 45th Street, Su. 2800  
New York, NY 10036  
[eshampnoi@srr.com](mailto:eshampnoi@srr.com)

Articles should be submitted in electronic document format (pdfs are NOT acceptable), and include biographical information.

[www.nysba.org/Inside](http://www.nysba.org/Inside)



## From Your Chapter President



It is once again my honor to welcome you to another year at the Risk Management Association. For our newest members, please let me extend a hearty welcome! And for our

longstanding members, we sincerely appreciate your support through the years.

As we embark on 2018, we are excited to introduce this newsletter to the Long Island chapter – a new member benefit. Each issue of the newsletter will contain an article on the topic of risk management, a list of upcoming events and member news. Knowing that our members lead busy lives, we plan on keeping the newsletter short and informative – with news you can use.

The Long Island Chapter has grown in a myriad of ways over the last several years. Our executive board has become very active and is currently comprised of professionals from a wide range of disciplines: bankers, lenders, advisors, accountants and, of course, attorneys. In recognition that we need to begin developing future Association leaders, we have a Young Professionals Committee. The YPC runs its own events and participates in ours. In addition, select members of the YPC participate in our board meetings, where they learn firsthand how our board operates.

As always, we strive to present programs and events that our members find valuable. We also aim to diversify the composition of our chapter to include participants from a wide range of industries and disciplines. To those ends, if there are topics you'd like us to address either in the newsletter or through a program, please let us know. And if you have a connection or colleague you think would be a good fit for our organization, we hope you will bring them to a meeting and show them what we're all about.

Wishing you a great 2018.

— Michael Heller

## Up next...

### CHAPTER EVENTS:

FEBRUARY 9	2018 Economic Outlook
APRIL 10	Educational Event: Lending to Construction Contractors
APRIL 20	Panel Discussion
JUNE 5	Networking Mixer

### YOUNG PROFESSIONALS COMMITTEE EVENTS:

FEBRUARY 23	Educational Event
MAY 3	Cinco de Mayo Event
JUNE 12	Nine and Dine

**DETAILS [HERE](#)**

## Approaching your Cybersecurity Risk

By Steven S. Rubin, Moritt Hock & Hamroff LLP

As the average cost of a data breach in the United States exceeds \$7 million, companies must prepare to mitigate such an incident or close their doors. Appropriate legal and technical preparation can help to reduce the adverse consequences of an attack. Currently, based on the nature of a company's business and the information it collects, a myriad of laws and regulations may apply. Failure to take appropriate steps to adequately come into compliance subjects a business to enforcement actions by agencies, lawsuits from affected consumers and fines from various state regulators.

Compliance with the number and complexity of federal and state cybersecurity laws and regulations is no simple task. As an essential part of a cybersecurity program and before a potential breach occurs, companies need to develop a

Written Information Security Policy ("WISP") and create a network of relationships with experts to contact in the event of a suspected breach. A WISP is an internal company document encompassing, among other things, the company's methodologies in identifying, protecting, detecting and responding to incidents. A WISP not only allows a company to identify and address potential compliance issues, but also incorporates legal principles to mitigate damages in the event of an incident. A WISP also provides guidance and procedures to each department on how it should handle information.

As the law develops, WISPs may become an industry best practice. A properly drafted WISP will require that a company's breach response be documented and will be consistent with evidentiary rules. In responding to an incident, a company should



know not only the appropriate information to preserve but also, how to maintain that information in an admissible format.

Legal counsel is an integral part of the WISP creation process. Utilization of legal advice in connection with the WISP creates an argument that at least some aspects of the process are shielded from disclosure in litigation because of the attorney-client privilege or attorney work product doctrines. If legal counsel played no role, information provided to a company from a computer security professional would most likely be discoverable in litigation.

The generation of a WISP may require the hiring of outside vendors as well as communication with different levels of staff hierarchy. All communications should include provisions explaining that the information is confidential and being gathered for the purpose of rendering legal advice.

Most businesses face complex and growing cybersecurity concerns. Risk management professionals can bring real value to their companies by addressing these concerns and reducing their companies' risks because cybersecurity is not limited to the technology group but requires a top-down organizational approach.

*Did You Know...*

## The Risk Management Association Scholarship Program

The Risk Management Association, LI Chapter offers scholarships to students in an undergraduate program who are interested in working in the banking industry after graduation.

The chapter is awarding scholarships ranging from \$1,500 to \$2,500.

For more information about the program, including criteria and deadlines, click [HERE](#).





# February meeting...

## 2018 Outlook on Economies and Markets

Friday, February 9, 2018

8:00 – 10:00am

Radisson Hotel

110 Vanderbilt Motor Parkway, Smithtown

Speaker:

Albert J. Brenner

Director of Asset Allocation Strategy

People's United Bank

Sponsored by:



REGISTRATION [HERE](#)



# Thank you...

TO OUR PREVIOUS SPONSORS:



## 2017-18 RMA-LI Board

### **PRESIDENT**

**Michael Heller**  
Rivkin Radler, LLP

### **SECRETARY**

**Richard Smith**  
The First National Bank of LI

### **TREASURER**

**Paul Becht**  
Margolin, Winer & Evens, LLP

### **VICE PRESIDENT**

**Richard Romano**  
Citibank, N.A.

### **ASSISTANT SECRETARY**

**Victoria Scolaro**  
Bank of America, N.A.

### **ASSISTANT TREASURER**

**Toni Badolato**  
People's United Bank

**Jennifer Acerra**  
Citibank, N.A.

**Matt Crennan**  
BNB Bank

**Barbara Liguori**  
Capital One Bank

**Joan Brigante**  
Retired People's United Bank

**Bonnie Dougherty**  
Valley National Bank

**Theresa McCarthy**  
BNB Bank

**Alison Burke**  
M&T Bank

**Barry Garfield**  
Garfield Consulting, LLC

**Robert Milas**  
Wells Fargo Bank

**Dan Castellano**  
Castellano Korenberg & Co.

**James Goldrick**  
NYBDC

**David Saunders**  
Signature Bank

**William Cimbol**  
TD Bank

**Marc Hamroff**  
Moritt Hock & Hamroff LLP

**Neil Seiden**  
Asset Enhancement Solutions, LLC

**Bill Conlan**  
HSBC Bank USA, N.A.

**Sylvia Kachala**  
Bank of America, N.A.

**Brian Stone**  
M&T Bank

**Peggy Coppola**  
Santander Bank

**David Katzman**  
M&T Bank

**Robin Wojciechowicz**  
Dime Community Bank

**Keith Lawlor**  
TD Bank

**ADMINISTRATOR**  
Connor Kachala

### **RMA YOUNG PROFESSIONALS COMMITTEE OFFICERS**

**Matthew Crennan**  
BNB Bank

**Michael Kid**  
Chase Bank

**Danielle McKenna**  
TD Bank

**Keith Annunziata**  
Sheehan & Company

For more information, [CLICK HERE](#) for the RMA-LI Website

# The Internet of Things: marrying cybersecurity with product liability litigation

By Steven Rubin  
and Julia Gavrilov

The Internet of Things (IoT) refers to objects which have network connectivity, allowing them to send and receive data. Examples include thermostats, baby monitors and medical devices. As the number of connected devices proliferates, so too will the risk that vulnerabilities will be exploited by hackers, implicating new cybersecurity issues. Developments relating to damages caused by the vulnerabilities of IoT devices demonstrate how creative plaintiffs are exploiting this new technology medium.

Malefactors are exploiting vulnerabilities in certain IoT devices that fail to have adequate cybersecurity measures, resulting in attacks that cause either physical damage or the theft of personal data. For example, ADT's home security system has been targeted in multiple suits on the basis that its wireless



systems allow hackers to, among other things, tamper with equipment and/or use customers' own security cameras to spy on them.

The next wave of IoT-related litigation will likely be in the context of a distributed denial of service attack (DDoS). For example, coffee makers

are hacked and then used to issue thousands of queries to a website, effectively making that website inaccessible or denying service from that site. In such instances, a plaintiff such as Macy's could sue for intangible damage caused by the inability of customers to access their website.

GGI member firm  
**Moritt Hock & Hamroff LLP**  
Law Firm Services  
Garden City, NY, United States  
T: +1 516 873 2000  
W: [www.morittthock.com](http://www.morittthock.com)  
**Steven Rubin**  
E: [srubin@morittthock.com](mailto:srubin@morittthock.com)  
**Julia Gavrilov**  
E: [jgavrilov@morittthock.com](mailto:jgavrilov@morittthock.com)



### Steven Rubin

**Steven Rubin** is a Partner at **Moritt Hock & Hamroff LLP (MHH)**, a full service, AV-rated law firm headquartered in Garden City, New York and providing representation in over 19



Julia Gavrilov

areas of discipline, where he serves as Chair of the firm's Patent Practice Group and as Co-Chair of its Cybersecurity Practice Group. **Julia Gavrilov** is an Associate in the Litigation Practice Group at MHH, specialising in com-

plex commercial and business litigation.



**Moritt Hock  
& Hamroff** LLP  
ATTORNEYS AT LAW



# **CYBER COVERAGE**

# **I.**

## **Coverage under Non-Cyber Policies**

SENTENCING GUIDELINES MANUAL § 2T4.1 (2009). Urbanski prepared a tax loss analysis that Morse submitted at his sentencing. Urbanski calculated the tax loss to be \$179,840. Consistent with Urbanski's analysis, the district court found the tax loss to be less than \$200,000 but greater than \$80,000, putting Morse at offense level 16 with a Guidelines range of 24 to 30 months. The court sentenced Morse within this range. Punishment in this case for conduct that was taken into account in Morse's 1999 sentence cannot be a violation of the Fifth Amendment because the earlier sentence was within the statutorily authorized punishment range. *See Witte*, 515 U.S. at 398–99, 115 S.Ct. 2199. Accordingly, the district court did not err in failing to reduce tax loss calculations to exclude tax losses already assessed against Morse.

### III.

For the reasons set forth, we affirm the judgment of the district court.



**EYEBLASTER, INC., Plaintiff–  
Appellant,**

**v.**

**FEDERAL INSURANCE COMPANY,  
Defendant–Appellee.**

**No. 08–3640.**

United States Court of Appeals,  
Eighth Circuit.

Submitted: June 10, 2009.

Filed: July 23, 2010.

**Background:** Insured internet advertising business brought declaratory judgment ac-

tion against liability insurer, seeking determination that it was entitled to coverage under a general liability insurance policy and a technology errors and omissions liability policy in lawsuit filed by third-party computer user. The United States District Court for the District of Minnesota, Ann D. Montgomery, J., 2008 WL 4539497, granted summary judgment in favor of insurer. Insured appealed.

**Holdings:** The Court of Appeals, John R. Gibson, Circuit Judge, held that:

- (1) general liability policy provided coverage;
- (2) impaired property exclusion in general liability policy did not bar coverage; and
- (3) errors and omissions policy provided coverage.

Reversed and remanded.

Colloton, Circuit Judge, filed opinion, concurring in the judgment.

### 1. Federal Courts ⇨776, 802

The court of appeals reviews the district court's grant of summary judgment de novo, viewing the facts in the light most favorable to the non-movant.

### 2. Federal Courts ⇨786

The court of appeals applies de novo review to the district court's interpretation of insurance policies, which is an issue of state law.

### 3. Insurance ⇨2913

Under Minnesota law, a liability insurer's duty to defend is distinct from and broader than its duty to indemnify the insured.

### 4. Insurance ⇨2913, 2939

Under Minnesota law, the burden is on the liability insurer to prove that it has

no duty to defend, and in so doing the insurer must show that each claim asserted in the lawsuit clearly falls outside the policy.

**5. Insurance ⇨2939**

Although a liability insurer's duty to defend is generally determined by comparing the allegations in the underlying complaint to the policy, under Minnesota law, if the insured presents facts that arguably demonstrate coverage or if the insurer becomes aware of such facts, the insurer then bears a heavy burden of proving that it has no such duty.

**6. Insurance ⇨2277**

Under Minnesota law, general liability insurance policy, which covered the loss of use of tangible property that was not physically injured, provided coverage to insured internet advertising business for lawsuit brought by third-party computer user, who alleged that his computer froze up, became inoperable, and crashed after he visited insured's website, and that his computer was no longer usable; the loss allegations in third-party lawsuit were within the scope of coverage for loss of use of tangible property.

**7. Insurance ⇨2120**

Under Minnesota law, an insured is entitled to have its case considered by the fact-finder once it has established a prima facie case of coverage.

**8. Insurance ⇨2290**

Under Minnesota law, the liability insurer has the burden to prove that an exclusion applies.

**9. Insurance ⇨2278(21)**

Under Minnesota law, exclusion in general liability insurance policy for "impaired property," defined as tangible property that could be restored to use by repair or removal of insured's product or

work, did not bar coverage for lawsuit brought against insured internet advertising business by third-party computer user, who alleged that his computer was damaged by and became unusable after he visited insured's website; the computer was not "impaired property," within meaning of exclusion, because there was no showing that the property could be restored or repaired, or that insured's product was incorporated into third-party's computer, and third party alleged that he unsuccessfully attempted to have computer repaired.

See publication Words and Phrases for other judicial constructions and definitions.

**10. Insurance ⇨2385**

Under Minnesota law, technology errors and omissions insurance policy, which covered loss from financial injury caused by unintentional wrongful act attributable to insured's product, provided coverage to insured internet advertising business for lawsuit brought by third-party computer user, who alleged that his computer became inoperable and no longer usable after insured installed tracking cookies, and other software on his computer; there was no evidence that insured's use of such products was intentionally wrongful, and consent judgment between third party and insured contained stipulation that insured did not act willfully or intentionally to injure him.

---

Robert Paul Thavis, argued Stephen H. Barrows, on the brief, Minneapolis, MN, for Appellant.

Dale Melvin Wagner, argued Jessica Schulte Williams, on the brief, Minneapolis, MN, for Appellee.

Before COLLOTON, JOHN R.  
GIBSON, and BEAM, Circuit Judges.

JOHN R. GIBSON, Circuit Judge.

Eyeblaster, Inc. (“Eyeblaster”) appeals from an adverse entry of summary judgment in its action against Federal Insurance Company (“Federal”) arising out of Federal’s denial of coverage under two insurance policies. A computer user sued Eyeblaster, alleging that Eyeblaster injured his computer, software, and data after he visited an Eyeblaster website. Eyeblaster tendered the defense of the lawsuit to Federal, seeking coverage under a General Liability policy and an Information and Network Technology Errors or Omissions Liability policy. Federal denied that it had a duty to defend Eyeblaster, and Eyeblaster brought this action seeking a declaration that Federal owed such a duty. The district court entered summary judgment in favor of Federal, and Eyeblaster appeals. We reverse.

Eyeblaster is a worldwide online marketing campaign management company that advertisers, advertising agencies, and publishers use to run campaigns across the Internet and other digital channels. Its primary product assists in the creation, delivery, and management of on-line interactive advertising. The company was established in 1999 and has fourteen offices worldwide, with six employees located in North America. In 2007, Eyeblaster delivered online marketing campaigns for nearly 7000 brand advertisers and served ads across more than 2700 global web publishers.

The industry in which Eyeblaster provides services is known as rich media advertising. Rich media allows customers to create interactive ads in a wide range of formats, and to track and manage the performance of the advertising campaigns.

Eyeblaster has the capacity to deliver ads simultaneously to billions of users globally and to constantly monitor its systems with network and system technicians and engineers. Its service uses cookies, which are typically used in the advertising industry to measure and enhance the effectiveness of an advertising campaign. It also uses JavaScript and Flash technology, which enliven web pages and increase the Internet’s utility. Eyeblaster does not use spyware or introduce malicious contact such as spam, viruses, or malware.

Eyeblaster purchased General Liability and Information and Network Technology Errors or Omissions insurance policies from Federal for the period from December 5, 2005 to December 5, 2007. Subject to the policies’ terms, Federal had a duty to defend Eyeblaster against lawsuits, even if such suits were false, fraudulent, or groundless.

David Sefton filed a lawsuit against Eyeblaster in Harris County, Texas in October 2006. Eyeblaster removed the action to federal court, where Sefton filed his First Amended Complaint the following month. Eyeblaster provided notice of and tendered defense of the First Amended Complaint to Federal in December 2006. On March 12, 2007, Federal sent Eyeblaster a letter denying all coverage. When Sefton amended his complaint a second time, Eyeblaster once again tendered defense of the suit to Federal, and again Federal denied coverage. Federal’s position was that it owed no coverage under the General Liability policy because Sefton did not assert claims for bodily injury caused by an occurrence, as defined by the policy. In addition, to the extent that Sefton alleged property damage, he did not allege that the property damage was caused by an accident or occurrence as the policy required. Federal also noted three exclu-

sions but offered no explanation as to why they would apply.

With respect to the Information and Network Technology Errors or Omissions coverage, Federal acknowledged that Sefton had complied with the requirement of claiming financial injury during the policy period. However, Federal claimed that Sefton had not alleged that Eyebaster committed a wrongful act (as defined by the policy) in connection with a product failure or in performing or failing to perform its service. Federal also pointed to general exclusionary language in the policy and to three specific exclusions.

In his Second Amended Complaint, Sefton alleges that his computer was infected with a spyware program from Eyebaster on July 14, 2006, which caused his computer to immediately freeze up. He further alleges that he lost all data on a tax return on which he was working and that he incurred many thousands of dollars of loss. Sefton hired a computer technician to repair the damage. Although he alleges that no repair was possible, he stated that his computer became operational again. Sefton asserted that he has experienced the following: numerous pop-up ads; a hijacked browser that communicates with websites other than those directed by the operator; random error messages; slowed computer performance that sometimes results in crashes; and ads oriented toward his past web viewing habits.

Sefton alleged violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Texas Business and Commercial Code §§ 48.052 and 48.101, a deceptive trade practice under Texas law, *prima facie* tort under Texas law, trespass, conversion, fraud, nuisance, invasion of privacy, intrusion upon seclusion, and conspiracy.

In stating these alleged violations, Sefton accused Eyebaster of intentionally accessing a protected computer without authorization, knowingly committing deceptive trade practice violations, intending to deceive Sefton, and intentionally installing unwanted spyware onto a user's computer.<sup>1</sup>

Eyebaster asserts that Federal knew of its business because Eyebaster completed an application to obtain professional liability insurance. Eyebaster disclosed to Federal that its core business activity is the technology used for interactive advertising content delivery and management, and any allegation that Eyebaster intentionally served an ad would have been in the ordinary course of its business. Eyebaster points out that it reasonably expected to be covered by Federal's policies at issue, and to suggest otherwise would reduce Federal's coverage to the point where it had no commercial justification.

The parties brought cross-motions for summary judgment. The district court granted Federal's motion and denied Eyebaster's, thus concluding the case in Federal's favor. The district court determined that Federal owed no duty to defend under either policy and, having made that decision, did not reach any of the exclusions.

Eyebaster asserts on appeal that the district court erred in failing to address coverage under the General Liability policy for "loss of use of tangible property that is not physically injured," and in failing to recognize that the Sefton complaint alleged "physical injury to tangible property." Eyebaster also asserts that the district court erred in determining that the Sefton complaint did not accuse Eyebaster of committing a "wrongful act" and that

1. Sefton dismissed his action against Eyebaster in December 2007 pursuant to a confi-

dential settlement.

Federal therefore owed no duty to defend under the Errors or Omissions policy.

I.

[1,2] We review the district court's grant of summary judgment de novo, viewing the facts in the light most favorable to Eyebaster, the non-movant. See *Northland Cas. Co. v. Meeks*, 540 F.3d 869, 872 (8th Cir.2008). We apply the same de novo review to the district court's interpretation of the insurance contracts at issue, *id.*, which is an issue of state law, *Meister v. W. Nat'l Mut. Ins. Co.*, 479 N.W.2d 372, 376 (Minn.1992). There is no dispute that the Federal policies are controlled by Minnesota law.

[3–5] Under Minnesota law, an insurer's duty to defend is distinct from and broader than its duty to indemnify the insured. *SCSC Corp. v. Allied Mut. Ins. Co.*, 536 N.W.2d 305, 316 (Minn.1995), *overruled on other grounds by Bahr v. Boise Cascade Corp.*, 766 N.W.2d 910 (Minn.2009). The burden is on the insurer to prove that it has no duty to defend, *SCSC Corp.*, 536 N.W.2d at 316, and in so doing the insurer must show that “each claim asserted in the lawsuit clearly falls outside the policy.” *Murray v. Greenwich Ins. Co.*, 533 F.3d 644, 648 (8th Cir.2008) (applying Minnesota law). Although the duty is generally determined by comparing the allegations in the underlying complaint to the policy, if the insured presents facts that arguably demonstrate coverage or if the insurer becomes aware of such facts, the insurer then bears a “heavy burden” of proving that it has no such duty. *Id.* at 648–49.

II.

The General Liability policy Eyebaster purchased from Federal obligates the insurer to provide coverage for property

damage caused by a covered occurrence. Property damage means “physical injury to tangible property, including resulting loss of use of that property . . . ; or loss of use of tangible property that is not physically injured.” The definition of “tangible property” excludes “any software, data or other information that is in electronic form.”

[6] The district court concluded that the Sefton complaint does not allege damage to tangible property because it only claims damage to software, which is by definition excluded. The district court relied on *America Online, Incorporated v. St. Paul Mercury Insurance Company*, 347 F.3d 89 (4th Cir.2003), in which America Online, Inc. (“AOL”) attempted to require its insurer to defend against claims that AOL's proprietary software package had “altered the customers' existing software, disrupted their network connections, caused them loss of stored data, and caused their operating systems to crash.” 347 F.3d at 93. The Fourth Circuit rejected AOL's argument because its insurance policy covered liability for “physical damage to tangible property,” and the court identified the configuration instructions, data, and information as intangible and abstract. *Id.* at 96. Eyebaster attempts to distinguish this portion of the AOL case without success. The Sefton complaint alleges direct injury to the operation of his computer, but it alleges no damage to the hardware itself. The complaint would have had to make a claim for physical injury to the hardware in order for Eyebaster to have coverage for “physical injury to tangible property.”

Eyebaster argues that the district court erred in failing to consider Federal's duty under the second part of the definition of “property damage,” which obligates the company to provide coverage if Eyebaster is alleged to have caused the “loss of use of

tangible property that is not physically injured.” The tangible property is Sefton’s computer, and Eyebaster points to language from the Sefton complaint in which he alleges his computer was “taken over and could not operate,” “froze up,” and would “stop running or operate so slowly that it will in essence become inoperable.” Sefton also alleges that he experienced “a hijacked browser—a browser program that communicates with websites other than those directed by the operator,” and “slowed computer performance, sometimes resulting in crashes.” Sefton asserts that his computer has three years of client tax returns that he cannot transfer because he believes the spyware files would also be transferred, and he therefore must reconstruct those records on a new computer. He thus argues that his computer is no longer usable, as he claims among his losses “the cost of his existing computer.”

Federal did not include a definition of “tangible property” in its General Liability policy, except to exclude “software, data or other information that is in electronic form.” The plain meaning of tangible property includes computers, and the Sefton complaint alleges repeatedly the “loss of use” of his computer. We conclude that the allegations are within the scope of the General Liability policy. See *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 207 F.Supp.2d 459, 470 (E.D.Va.2002) (district court found loss of use of tangible property when complaint alleged that AOL caused loss of use of computers and computer functionality, but concluded no coverage existed because allegations were otherwise excluded), *aff’d*, 347 F.3d 89 (4th Cir.2003); *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1113, 1116 (W.D.Okla.2001) (in case with “property damage” language identical to language of Eyebaster policy, court holds that “[b]ecause a computer clearly is tangi-

ble property, an alleged loss of use of computers constitutes ‘property damage’ within the meaning of plaintiff’s policy”).

[7,8] Federal argues that, even if it owes a duty to defend because Sefton alleged a loss of use of tangible property, that coverage is barred by the exclusion for Impaired Property/Property Not Physically Injured. Under Minnesota law, an insured is entitled to have its case considered by the fact-finder once it has established a prima facie case. The insurer then has the burden to prove that an exclusion applies. *SCSC Corp. v. Allied Mut. Ins. Co.*, 536 N.W.2d 305, 313 (Minn. 1995), *overruled on other grounds by Bahr v. Boise Cascade Corp.*, 766 N.W.2d 910 (Minn.2009). Exclusions are narrowly interpreted against the insurer. *SCSC Corp.*, 536 N.W.2d at 314.

[9] Federal points to an exclusion in the General Liability policy entitled “Damage to Impaired Property or Property Not Physically Injured,” which states that the insurance does not apply to property damage to impaired property or property that has not been physically injured if the damage arises out of any defect, deficiency, inadequacy, or dangerous condition in Eyebaster’s product or work. “This exclusion does not apply to the loss of use of other tangible property resulting from sudden and accidental physical injury to your product or your work after it has been put to its intended use.” The policy also defines “impaired property:”

Impaired property means tangible property, other than your product or your work, that cannot be used or is less useful because:

- it incorporates your product or your work that is known or thought to be defective, deficient, inadequate or dangerous; or



- you have failed to fulfill the terms or conditions of a contract or agreement; if such property can be restored to use by;
- the repair, replacement, adjustment or removal of your product or your work; or
- your fulfilling the terms or conditions of the contract or agreement.

Federal asserts that, if Sefton lost the use of his hardware, it would be “impaired property.” It also asserts that Sefton’s computer would be “property not physically injured” because it was damaged by the allegedly defective and dangerous condition in Eyeblaster’s software.

We conclude that Federal has not met its burden of proving that the exclusion applies. Sefton’s computer cannot be considered “impaired property” because no evidence exists that the computer can be restored to use by removing Eyeblaster’s product or work from it. The record shows that Eyeblaster provides advertising services to its clients to enable those clients to reach and interact with online computer users such as Sefton. It is not clear that an Eyeblaster product or Eyeblaster’s work ever existed on Sefton’s computer, and thus it is equally unclear that such product or work could be removed from the computer. Sefton alleges that the website that he believes caused the damage to his computer “was owned and operated by Eyeblaster or person’s [sic] or entities that are controlled directly or indirectly by Eyeblaster.” Such a broad characterization does not suffice to satisfy the requirement that Eyeblaster incorporated its product or work into Sefton’s computer.

Even if the Sefton complaint could be read to meet the first part of the definition of “impaired property,” Sefton alleges that he unsuccessfully attempted to have the damage to his computer repaired. Federal

thus cannot demonstrate that Sefton’s computer could be restored by the removal of Eyeblaster’s product or work. See *Corn Plus Coop. v. Cont’l Cas. Co.*, 444 F.Supp.2d 981, 990 (D.Minn.2006) (applying Minnesota law to identical exclusionary language, court holds that repair and replacement of defective welds in piping system cannot restore damaged product running through the system and thus does not fall within definition of “impaired property,” citing cases from other jurisdictions).

Federal suggests that two more exclusions to its General Liability policy apply. The first is the “Expected Or Intended Injury” exclusion, which precludes coverage for property damage arising out of an act that is intended by the insured or that would be expected from the standpoint of a reasonable person in the circumstances of the insured to cause property damage. The second is the “Intellectual Property Laws Or Rights” exclusion, which excludes damages related to infringement or violation of any intellectual property law or right. Federal advances no convincing argument in favor of either, and we conclude that these exclusions likewise do not apply.

### III.

[10] Eyeblaster next asserts that the district court erred by concluding that the Sefton complaint does not allege a cause of action covered by Federal’s Information and Network Technology Errors or Omissions policy. The policy obligates Federal to pay loss for financial injury caused by a wrongful act that results in the failure of Eyeblaster’s product to perform its intended function or to serve its intended purpose. “Financial injury” is defined as economic injury resulting from property that cannot be used or is less useful. As the name of the policy suggests, the Errors or Omissions policy specifically covers intan-

gible property such as software, data, and other electronic information. Under the policy, a “wrongful act” is an error, an unintentional omission, or a negligent act.

Federal concedes that Sefton’s complaint does allege a “financial injury,” which the district court acknowledged. However, the district court determined that the Sefton complaint does not claim a “wrongful act” because the complaint alleges that Eyebaster acted intentionally in placing its software on Sefton’s computer. The district court rejected Eyebaster’s argument that the policy covers allegedly intended acts resulting in unintended injuries, and concluded that the “substance of the allegations” is that Eyebaster intended to place its product on Sefton’s computer.

Recognizing that Minnesota law places the burden on the insurer to prove that it has no duty to defend, and in so doing it must show that “each claim asserted in the lawsuit clearly falls outside the policy,” *Murray v. Greenwich Ins. Co.*, 533 F.3d 644, 648 (8th Cir.2008), we conclude that Federal owes a duty under its Errors or Omissions policy.

The Sefton complaint is lengthy and contains many, many allegations. Both parties can selectively cite words and phrases to support their arguments. However, under the appropriate standard of review, Federal cannot demonstrate that each claim in the Sefton complaint falls outside the coverage of its Errors or Omissions policy. This court has defined “error” in a technology errors and omissions policy to include intentional, non-negligent acts but to exclude intentionally wrongful conduct. *St. Paul Fire & Marine Ins. Co. v. Compaq Computer Corp.*, 539 F.3d 809, 815 (8th Cir.2008). Sefton alleges that Eyebaster installed tracking cookies, Flash technology, and JavaScript on his computer, all of which are intentional acts. How-

ever, Federal can point to no evidence that doing so is intentionally wrongful. As Eyebaster points out in an affidavit filed with the district court, Federal’s parent company utilizes JavaScript, Flash technology, and cookies on its own website. Federal cannot label such conduct as intentionally wrongful merely because it is included in the Sefton complaint; Federal has a duty to show that the use of such technology is outside its policy’s coverage. Federal points to no evidence that the allegations concerning tracking cookies, etc. spoke of intentional acts that were either negligent or wrongful. Under *St. Paul*, therefore, the Sefton complaint does allege a wrongful act.

The record also contains the Consent Judgment and Permanent Injunction entered by the United States District Judge in the Sefton action, which includes the following stipulation:

Sefton acknowledges that after a review of the evidence supplied in discovery, he had no basis in fact to allege that [Eyebaster] had acted willfully, intentionally, or otherwise with malice aforethought, to injure him or his business or to violate any laws and accordingly he is now willing to submit himself . . . to the within permanent injunction against pursuing claims like those asserted in this case against [Eyebaster].

While the Consent Judgment and Permanent Injunction obviously did not exist until the Sefton lawsuit was concluded, the quoted language serves to confirm that Eyebaster’s use of technology was subject to coverage under Federal’s Errors or Omissions policy. Under Minnesota law, if the insured presents facts that arguably demonstrate coverage or if the insurer becomes aware of such facts, the insurer then bears a “heavy burden” of proving that it has no duty to defend. *Murray*, 533 F.3d at 648–49 (internal quotation

marks omitted). Federal did not meet that burden.

Just as with the General Liability policy, Federal argues that several exclusions would apply if we were to conclude that coverage exists under the Errors or Omissions policy. Those exclusions speak of intentional conduct that Federal has not carried its burden to show.

#### IV.

For the foregoing reasons, we reverse the district court judgment and remand for further proceedings.

COLLTON, Circuit Judge, concurring in the judgment.

I agree, substantially for the reasons stated by the court, that Federal Insurance Company has not established that all parts of David Sefton's claims against Eyebaster, Inc., fall clearly outside the scope of coverage provisions under the General Liability and Errors or Omissions policies that Eyebaster purchased from Federal, although I would not rely on the consent judgment cited by the court, *ante*, at 804-05, because it did not exist at the time of Federal's disputed denial. I do not join the court's conclusion about exclusions under the General Liability policy. While I agree that Sefton's computer is not "impaired property" for purposes of the first exclusion, the computer is "property that has not been physically injured"—indeed, the court concludes elsewhere that the computer is "tangible property that is not physically injured." *Ante*, at 801. And it is likely that Sefton's complaint should be read to allege that the damage to his computer arose out of a dangerous condition in Eyebaster's product or work, thus satisfying the second criterion for the exclusion. I do agree, however, that there is no applicable exclusion that bars coverage under the Errors or Omissions policy. Because

an insurer's duty to defend arises when *any part* of the claim against the insured is arguably within the scope of coverage afforded by the policy, *Metro. Prop. & Cas. Ins. Co. v. Miller*, 589 N.W.2d 297, 299 (Minn.1999), I agree that Federal had a duty to defend. Therefore, I concur in the judgment.



UNITED STATES of America,  
Appellee,

v.

Thomas Dewayne ROSS, also known as  
Thomas Dwayne Ross, also known as  
Dewayne Ross, also known as Wayne,  
Appellant.

No. 09-3879.

United States Court of Appeals,  
Eighth Circuit.

Submitted: May 14, 2010.

Filed: July 23, 2010.

**Background:** Defendant pleaded guilty, in the United States District Court for the District of Nebraska, Richard G. Kopf, J., to conspiracy to distribute cocaine base. He appealed his sentence.

**Holding:** The Court of Appeals, Colloton, Circuit Judge, held that defendant's prior Nebraska conviction for attempted burglary constituted a conviction for a crime of violence within meaning of the Sentencing Guidelines' career offender provisions.

Affirmed.

**LIBERTY CORPORATE CAPITAL  
LIMITED, Plaintiff,**

**v.**

**SECURITY SAFE OUTLET,  
INC., et al., Defendants.**

**Civil Action No. 5:12-cv-178-KSF.**

United States District Court,  
E.D. Kentucky,  
Central Division at Lexington.

March 27, 2013.

**Background:** Insurer filed action for declaratory judgment that it was not obligated under commercial general liability (CGL) policy to defend or indemnify insured, a business that sold firearms, or insured's employee, a former information technology (IT) employee for competitor, in competitor's underlying action against insured for misappropriation of trade secrets, i.e., competitor's customer database, including customer names and email addresses, and related claims. Insurer filed motion for summary judgment.

**Holdings:** The District Court, Karl S. Forester, Senior District Judge, held that:

- (1) underlying claim did not involve tangible property, for coverage purposes, and
- (2) exclusion from coverage for advertising injury was applicable.

Motion granted.

**1. Federal Civil Procedure** ⇨2466,  
2470.4

In reviewing a motion for summary judgment, the district court must determine whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law. Fed.Rules Civ.Proc.Rule 56(a), 28 U.S.C.A.

**2. Federal Civil Procedure** ⇨2546

To withstand a motion for summary judgment, the mere existence of a scintilla

of evidence in support of the nonmoving party's position will be insufficient; there must be evidence on which the jury could reasonably find for the nonmoving party, and if the evidence is merely colorable, or is not significantly probative, summary judgment may be granted. Fed.Rules Civ. Proc.Rule 56(a), 28 U.S.C.A.

**3. Federal Courts** ⇨382.1

In exercising diversity jurisdiction, the district court must apply state law in accordance with controlling decisions of the highest state court.

**4. Insurance** ⇨1863

Under Kentucky law, interpretation and construction of an insurance contract is a matter of law for the court.

**5. Insurance** ⇨1835(2), 2098

Under Kentucky law, exclusions in insurance policies are to be narrowly interpreted and all questions resolved in favor of the insured.

**6. Insurance** ⇨1832(1), 2090

Under Kentucky law, any doubt as to the coverage or terms of an insurance policy should be resolved in favor of the insured.

**7. Insurance** ⇨1829

Under Kentucky law, since the insurance policy is drafted in all details by the insurance company, it must be held strictly accountable for the language used.

**8. Insurance** ⇨1805, 1812, 1822

Under Kentucky law, an insurance policy is to be read according to its plain meaning, its true character and purpose, and the intent of the policy.

**9. Insurance** ⇨1812, 1816, 1822, 1832(1,  
2)

Under Kentucky law, the rule of strict construction of an insurance policy against an insurance company does not mean that

every doubt must be resolved against it and does not interfere with the rule that the policy must receive a reasonable interpretation consistent with the parties' object and intent or narrowly expressed in the plain meaning and/or language of the contract, nor should a nonexistent ambiguity be utilized to resolve a policy against the company.

**10. Insurance ⇌1807**

Under Kentucky law, courts should not rewrite an insurance contract to enlarge the risk to the insurer.

**11. Insurance ⇌1721, 1809**

Under Kentucky law, when the terms of an insurance contract are unambiguous and not unreasonable, they will be enforced.

**12. Insurance ⇌1822, 1827, 1836, 2098**

Under Kentucky law, while exceptions and exclusions in insurance policies are to be narrowly construed to effectuate insurance coverage, this strict construction should not overcome plain clear language, resulting in a strained or forced construction.

**13. Insurance ⇌1725, 2098**

Under Kentucky law, reasonable conditions, restrictions, and limitations on insurance coverage are not deemed per se to be contrary to public policy.

**14. Insurance ⇌2268, 2913**

Under Kentucky law, an insurer's duty to defend is broader than the duty to indemnify, and consequently, if there is no duty to defend, then there is no duty to indemnify.

**15. Insurance ⇌2914**

Under Kentucky law, a court should determine at the outset of litigation whether an insurance company has a duty to defend its insured by comparing the allegations in the underlying complaint with the terms of the insurance policy, and an insurance company has a duty to defend

its insured if the language of an underlying complaint against the insured brings the action within the scope of the insurance contract.

**16. Insurance ⇌2277**

Insured's alleged misappropriation of trade secrets under Kentucky law, relating to email addresses for customers of competitor in the business of selling firearms, which addresses the insured's information technology (IT) employee, who previously had worked for competitor, allegedly had obtained from electronic backup copy of competitor's customer database, did not involve "tangible property," within meaning of commercial general liability (CGL) policy's coverage for physical damage to tangible property; email addresses had no physical form or characteristics.

**17. Insurance ⇌2277**

Insured's alleged misappropriation of trade secrets under Kentucky law, relating to email addresses for customers of competitor in the business of selling firearms, which addresses the insured's information technology (IT) employee, who previously had worked for competitor, allegedly had obtained from electronic backup copy of competitor's customer database, involved "electronic data," within meaning of commercial general liability (CGL) policy's electronic data exclusion from definition of covered property damage; exclusion defined electronic data as information stored, created, or used on computer software.

See publication Words and Phrases for other judicial constructions and definitions.

**18. Insurance ⇌1809**

Under Kentucky law, where the terms of an insurance policy are clear and unambiguous, the policy will be enforced as written.

**19. Insurance ⇨2303(1)**

Even assuming that insured's alleged misappropriation of trade secrets under Kentucky law, relating to email addresses for customers of competitor in the business of selling firearms, which addresses the insured's information technology (IT) employee, who previously had worked for competitor, had allegedly obtained from electronic backup copy of competitor's customer database, and which were used by insured to solicit competitor's customers, constituted advertising injury for purposes of commercial general liability (CGL) policy's advertising injury coverage, policy's exclusion for advertising injury arising out of breach of contract was applicable; competitor's underlying complaint alleged that IT employee's disclosure of email addresses to insured violated the terms of his non-compete agreement with competitor, and without this alleged breach of contract, insured would not have had the email addresses.

**20. Insurance ⇨2277**

Alleged harm to the identity, reputation, and goodwill of a competitor of the insured in the business of selling firearms, from insured's trademark infringement by continuing to use the mark as the name of its business after insured's tradename license agreement with competitor allegedly had terminated because insured had breached it, did not involve "tangible property," within meaning of commercial general liability (CGL) policy's coverage for physical damage to tangible property; identity, reputation, and goodwill had no physical form and characteristics. Lanham Act, § 43, 15 U.S.C.A. § 1125.

See publication Words and Phrases for other judicial constructions and definitions.

**21. Insurance ⇨2302**

Commercial general liability (CGL) policy's exclusion from advertising injury coverage, for injury arising out of trade-

mark infringement, applied to insured's alleged trademark infringement by continuing to use the mark as the name of its business after insured's tradename license agreement with competitor in the business of selling firearms allegedly had terminated because insured had breached it, though competitor's underlying complaint alleged that insured's use of the mark disparaged competitor's good will. Lanham Act, § 43, 15 U.S.C.A. § 1125.

**22. Insurance ⇨1772, 2098**

Under Kentucky law, exclusions from insurance coverage that are unequivocally conspicuous, plain, and clear will be enforced.

**23. Trademarks ⇨1062**

Trademarks and trade dress are separate and distinct causes of action under the Lanham Act. Lanham Act, §§ 43, 45, 15 U.S.C.A. §§ 1125, 1127.

**24. Trademarks ⇨1063**

"Trade dress" is the design or packaging of a product which has acquired a secondary meaning sufficient to identify the product with its manufacturer or source.

See publication Words and Phrases for other judicial constructions and definitions.

**25. Insurance ⇨1817, 1820, 1832(1, 2)**

Under the reasonable expectations doctrine recognized by Kentucky law, ambiguous terms in an insurance contract must be interpreted in favor of the insured's reasonable expectations and construed as an average person would construe them, but, only actual ambiguities, not fanciful ones, will trigger application of the doctrine.

**26. Insurance ⇨1808, 1832(2)**

Under Kentucky law, a non-existent ambiguity should not be utilized to resolve an insurance policy against an insurer, and

it is not enough for one party to claim ambiguity; the mere fact that a party attempts to muddy the water and create some question of interpretation does not necessarily create an ambiguity.

#### 27. **Contracts** ⇐143(2)

Under Kentucky law, a contract is “ambiguous” if a reasonable person would find it susceptible to different or inconsistent interpretations.

See publication Words and Phrases for other judicial constructions and definitions.

#### 28. **Insurance** ⇐2098

Under Kentucky law, each exclusion in an insurance policy is to be read independently of every other exclusion, and if any one exclusion applies, there should be no coverage, regardless of inferences that might be argued on the basis of exceptions or qualifications contained in other exclusions.

---

B. Scott Jones, Justin Nathaniel Rost, Danielle J. Ravencraft, Reminger Co., L.P.A., Louisville, KY, Gregory L. Mast, Kylie Holladay, Paul L. Fields, Jr., Fields Howell, Atlanta, GA, for Plaintiff.

Carroll M. Redford, III, Don A. Pisacano, Miller, Griffin & Marks, P.S.C., William L. Montague, Jr., Montague Law, PLLC, Lexington, KY, for Defendants.

### **OPINION & ORDER**

KARL S. FORESTER, Senior District Judge.

This matter is before the court on the motion of Plaintiff, Liberty Corporate Capital Limited (“Liberty”), for summary judgment [DE # 37]. The motion having been fully briefed, this matter is ripe for review. Although Liberty has requested oral argument on its motion, this request

will be denied, as the Court sees no need for oral argument.

### **I. FACTUAL BACKGROUND**

This case stems from an underlying case filed by Budsgunshop.com, LLC (“BGS”) against Defendants Security Safe Outlet, Inc. d/b/a Bud’s Gun Shop (“SSO”) and Matthew Denninghoff, in which BGS alleges that SSO and Denninghoff misappropriated BGS’s trade secrets by improperly accessing BGS’s customer database and obtaining and using confidential customer information, including customer email addresses, for their commercial benefit [*Budsgunshop.com, LLC v. Security Safe Outlet, Inc., et al.*, Case # 5:10-cv-390, pending in the United States District Court, Eastern District of Kentucky]. Pursuant to insurance policies issued by Liberty to SSO, SSO seeks a defense and indemnity for itself and Denninghoff with respect to the claims alleged against them by BGS. Liberty has filed the instant declaratory judgment action, seeking a declaratory judgment that, under the policies at issue, Liberty is not obligated or required to indemnify and defend SSO or Denninghoff against the claims made against them by BGS in the underlying litigation and, further, that Liberty has no other obligation or duty to either BGS, Marion E. Wells, Jr., Rex McClanahan, or any other party, arising out of the claims made in the underlying litigation. Liberty has now filed a motion for summary judgment in its declaratory judgment action.

#### *A. The Underlying Lawsuit*

In order to consider Liberty’s motion for summary judgment, a brief explanation of the claims made by BGS in the underlying litigation is required. According to BGS’s second amended complaint, SSO was formed in June 2000 by Wells, with Wells as the sole shareholder [5:10-cv-390, DE

# 73]. Under the name “Bud’s Gun Shop,” SSO operated a retail store in Paris, Kentucky, selling security safes, firearms and related accessories. Around February 2007, Wells and Earley M. Johnson, II entered into a Stock Purchase Agreement whereby Johnson purchased a minority interest in SSO. In May 2007, Wells and McClanahan formed BGS for the purpose of selling firearms and related goods over the internet.

In April 2009, pursuant to a Stock Redemption Agreement entered into by Wells and Johnson, Johnson gained control of SSO through a buy-out of Wells’ interest in the company. As part of that transaction, SSO transferred its federal and state trademark rights in the tradename “Bud’s Gun Shop,” as well as variations of that name, to Wells. Pursuant to a Tradename License Agreement (the “Tradename License Agreement”), Wells then licensed back those rights on a limited basis to SSO to be used solely for a retail firearms store physically located in Paris, Kentucky, and/or a shooting or firing range business. According to BGS, because the parties anticipated that BGS would maintain the exclusive use of these rights in connection with its online retail business, these rights were not licensed to SSO for use in connection with the online sale of firearms. Wells has since assigned this License to BGS, along with the unregistered “Bud’s Gun Shop” trademark. Section 2 of the License provides that SSO’s use of the tradename shall discontinue if, over any one calendar month period during the term of the License, SSO’s over-the-counter sales of firearms from its retail store comprise less than 85% of SSO’s total sales of firearms for that month. The License further provides that, should SSO breach or fail to comply with any of the terms of Section 2 of the License, the License shall immediately terminate and SSO shall cease using the tradename. BGS alleges that SSO’s over-the-counter sales of fire-

arms from its retail store have comprised less than 85% of SSO’s total sales of firearms in one or more months since the License was executed, thereby causing a breach and immediate termination of the License. BGS further alleges that SSO has knowingly continued to use the “Bud’s Gun Shop” mark in a variety of ways to promote its business with its suppliers and the consuming public, notwithstanding the termination of the license.

After the April 2009 transaction, BGS and SSO continued to maintain a business relationship, pursuant to which BGS would use SSO as one of its suppliers to fulfill online orders. In order to obtain customer and order information necessary to fill specific orders, SSO was provided with limited access and limited authorization to BGS’s computer network system. SSO disputes whether its access and authorization to BGS’s computer network system was as “limited” as alleged by BGS.

Prior to January 2010, Denninghoff was an employee of BGS, working on information technology matters and in the coding, design, and implementation of BGS’s website. In January 2010, Denninghoff quit his job with BGS and began working with SSO. SSO’s Vice-President is Denninghoff’s sister, Jennifer Arnett. BGS alleges that, before quitting his job at BGS, Denninghoff erased the entire contents of the hard drive of the computer that BGS had provided to him and informed BGS that he would return only the hardware and software initially provided by BGS. Despite hiring a third party computer forensics expert to attempt to retrieve the deleted contents of Denninghoff’s work computer, BGS alleges that it has been unable to recover the contents of the hard drive. BGS also asked Denninghoff to provide the source code and other work product he created while a BGS employee. However, BGS alleges that Denninghoff indicated that the work product belonged



to him, his source code was stored on his own personal server and he provided only a marginally useful computer code to BGS. BGS alleges that it was required to hire another third party contractor to reconstruct the incomplete computer code into a workable program.

In April 2010, BGS learned that SSO was launching an online presence for the purpose of selling firearms and related goods over the internet, thereby placing the two companies in direct competition. Upon learning this information, BGS terminated all access by SSO to BGS's computer network system. However, beginning in September 2010, SSO began sending mass emails to BGS's customers regarding its new competing firearms business. BGS alleges that, in order to do so, SSO and Denninghoff improperly obtained BGS's customer's email addresses from BGS's customer database. Specifically, BGS alleges that it has discovered that, despite erasing the contents of his work computer, Denninghoff secretly kept much of the data from his work computer, as well as numerous backup copies of BGS's customer database from various backup dates, in his possession. According to BGS, SSO and Denninghoff used this information to obtain BGS's customer's email addressees.<sup>1</sup>

Based on these allegations, BGS alleges the following counts: (1) Count I—misappropriation of trade secrets in violation of K.R.S. §§ 365.880, *et seq.*; (2) Count II—

violation of the Lanham Act, 15 U.S.C. § 1125; (3) Count III—breach of contract—Tradename License; (4) Count IV—breach of fiduciary duty (against Denninghoff); (5) Count V—aiding and abetting breach of fiduciary duty (against SSO); (6) Count VI—breach of contract—non-compete agreement (against Denninghoff); (7) Count VII—tortious interference with contract (against SSO); (8) Count VIII—violation of 18 U.S.C. § 1030(a)(2) (the “Computer Fraud and Abuse Act”); (9) Count IX—violation of 18 U.S.C. § 1030(a)(4); (10) Count X—violation of K.R.S. § 434.845 (unlawful access of computer); and (11) Count XI—violation of K.R.S. § 434.855 (misuse of computer information) [5:10-cv-390, DE # 73]. The underlying litigation between BGS, SSO and others is currently pending in this Court.

#### B. *Liberty's Declaratory Judgment Action*

From approximately 2008 through 2012, SSO purchased a series of commercial general liability coverage policies from Liberty.<sup>2</sup> Each of these policies provided certain commercial general liability coverage to SSO, pursuant to specified terms, conditions and exclusions. On October 21, 2011, SSO made a claim for coverage under one or more of these policies seeking a defense and indemnity for both SSO and Denninghoff with regard to the claims made against them by BGS in the underlying lawsuit.<sup>3</sup> On June 1, 2012, Liberty filed its

1. SSO and Denninghoff do not dispute that Denninghoff provided the backup copies of BGS's database to SSO and that SSO used BGS's database in its entirety to send out email advertising “blasts” to the email addresses contained in the database. Rather, SSO and Denninghoff maintain that SSO was entitled to do so. [DE # 38 at p. 3].

2. Specifically, the following policies are relevant to this litigation: Policy Nos. L200805866, effective September 27, 2008,

through September 27, 2009; L201005866, effective September 27, 2010, through September 27, 2011; L201105866, effective September 27, 2011, through September 27, 2012 (collectively “Policies”); and Policy No. 200905866, effective September 27, 2009, through September 27, 2010 (the “2009 Policy”).

3. According to Liberty, because of the manner in which SSO and Denninghoff sought coverage, it is not clear which specific policy or

complaint in the instant case, seeking a declaratory judgment that no coverage exists under the Policy for SSO's insurance claim. Liberty has now filed a motion for summary judgment in its declaratory judgment action.

## II. STANDARD OF REVIEW

[1] Under Rule 56(a) of the Federal Rules of Civil Procedure, summary judgment is proper "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." See *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). In reviewing a motion for summary judgment, "this Court must determine whether 'the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law.'" *Patton v. Bearden*, 8 F.3d 343, 346 (6th Cir.1993) (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 251-52, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986)). The evidence, all facts, and any inferences that may permissibly be drawn from the facts must be viewed in the light most favorable to the nonmoving party. *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 587, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986).

[2] Once the moving party shows that there is an absence of evidence to support the nonmoving party's case, the nonmoving party must present "significant probative evidence" to demonstrate that "there is [more than] some metaphysical doubt as to

the material facts." *Moore v. Philip Morris Companies, Inc.*, 8 F.3d 335, 340 (6th Cir.1993). Conclusory allegations are not enough to allow a nonmoving party to withstand a motion for summary judgment. *Id.* at 343. "The mere existence of a scintilla of evidence in support of the [nonmoving party's] position will be insufficient; there must be evidence on which the jury could reasonably find for the [nonmoving party]." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. at 252, 106 S.Ct. 2505. "If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted." *Id.* at 249-50, 106 S.Ct. 2505 (citations omitted).

## III. ANALYSIS

### A. Applicable Law

[3-11] In exercising diversity jurisdiction in this case, the court must apply state law in accordance with controlling decisions of the highest state court. *Bailey Farms, Inc. v. NOR-AM Chem. Co.*, 27 F.3d 188, 191 (6th Cir.1994). Under Kentucky law, interpretation and construction of an insurance contract is a matter of law for the court. *Kemper v. Heaven Hill Distilleries*, 82 S.W.3d 869, 871 (Ky.2002). According to the Kentucky Supreme Court:

[A]s to the manner of construction of insurance policies, Kentucky law is crystal clear that exclusions are to be narrowly interpreted and all questions resolved in favor of the insured. Exceptions and exclusions are to be strictly construed so as to render the insurance effective. Any doubt as to the coverage or terms of a policy should be resolved in favor of the insured. And since the policy is drafted in all details

policies are at issue. However, Liberty contends (and SSO and Denninghoff do not dispute) that this issue need not be resolved, as the substantive provisions of the policies at

issue are identical. Accordingly, the parties both refer to the policies collectively as the "Policy." Following the parties' lead, the Court will do the same.

by the insurance company, it must be held strictly accountable for the language used.

*Eyler v. Nationwide Mut. Fire Ins. Co.*, 824 S.W.2d 855, 859–60 (Ky.1992) (citations omitted). However, such canons are applicable only “when the language of the insurance contract is ambiguous or self-contradictory. Otherwise, the contract is to be read according to its plain meaning, its true character and purpose, and the intent of the policies.” *Peoples Bank & Trust Co. v. Aetna Casualty & Surety Co.*, 113 F.3d 629, 636 (6th Cir.1997). Indeed, as noted by the Kentucky Supreme Court:

The rule of strict construction against an insurance company certainly does not mean that every doubt must be resolved against it and does not interfere with the rule that the policy must receive a reasonable interpretation consistent with the parties’ object and intent or narrowly expressed in the plain meaning and/or language of the contract. Neither should a nonexistent ambiguity be utilized to resolve a policy against the company. We consider that courts should not rewrite an insurance contract to enlarge the risk to the insurer. *U.S. Fidelity & Guar. Co. v. Star Fire Coals, Inc.*, 856 F.2d 31 (6th Cir.1988).

*St. Paul Fire & Marine Ins. Co. v. Powell-Walton-Milward, Inc.*, 870 S.W.2d 223, 226–227 (Ky.1994). Thus, “[w]hen the terms of an insurance contract are unambiguous and not unreasonable, they will be enforced.” *Kentucky Ass’n of Counties All Lines Fund Trust v. McClendon*, 157 S.W.3d 626, 630 (Ky.2005).

[12, 13] As noted above, exceptions and exclusions in insurance policies are to be narrowly construed to effectuate insurance coverage. However, this strict construction should not overcome “plain clear lan-

guage resulting in a strained or forced construction.” *Kemper*, 82 S.W.3d at 873–874 (quoting *Diamaco, Inc. v. Aetna Casualty & Surety Co.*, 97 Wash.App. 335, 983 P.2d 707 (1999)). “Reasonable conditions, restrictions and limitations on insurance coverage are not deemed *per se* to be contrary to public policy.” *Snow v. West American Ins. Co.*, 161 S.W.3d 338, 341 (Ky.App.2004).

[14, 15] In Kentucky, an insurer’s duty to defend is broader than the duty to indemnify. *James Graham Brown Foundation, Inc. v. St. Paul Fire & Marine Ins.*, 814 S.W.2d 273, 280 (Ky.1991).<sup>4</sup> “Under Kentucky law, a court should determine at the outset of litigation whether an insurance company has a duty to defend its insured by comparing the allegations in the underlying complaint with the terms of the insurance policy.” *Westfield Ins. Co. v. Tech Dry, Inc.*, 336 F.3d 503, 507 (6th Cir.2003). See also *Lenning v. Commercial Union Ins. Co.*, 260 F.3d 574, 581 (6th Cir.2001). “An insurance company has a duty to defend its insured if the language of an underlying complaint against the insured brings the action within the scope of the insurance contract.” *Westfield Ins. Co.*, 336 F.3d at 507. See also *DiBeneditto v. Medical Protective Co.*, 3 Fed.Appx. 483, 485 (6th Cir.2001) (unpublished) (“Kentucky courts have made it clear that allegations in a complaint are not by themselves sufficient to trigger the duty to defend, but rather, the obligation to defend arises out of the language of the insurance contract.”) (citing *Thompson v. West American Ins. Co.*, 839 S.W.2d 579, 581 (Ky.Ct.App.1992)) (other citations omitted); *James Graham Brown Foundation, Inc.*, 814 S.W.2d at 279–280 (Ky.1991) (“The insurer has a duty to defend if there

4. Consequently, if there is no duty to defend, then there is no duty to indemnify. *Nautilus Ins. Co. v. Structure Builders & Riggers Ma-*

*chinery Moving Division, LLC*, 784 F.Supp.2d 767, 771 (E.D.Ky.2011).

is any allegation which potentially, possibly or might come within the coverage of the policy. The insurance company must defend any suit in which the language of the complaint would bring it within the policy coverage regardless of the merit of the action.”) (citations omitted). Thus, the Court must closely examine both the language of BGS’s complaint and the language of the Policy to determine whether coverage exists in this case.

#### B. *Applicable Policy Provisions*

The Policy contains a grant of coverage as to liability for “property damage.” Under the Policy, “property damage” is defined as follows:

28. “Property Damage” means:

- a. Physical injury to tangible property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
- b. Loss of use of tangible property that is not physically injured. All such loss of use shall be deemed to occur at the time of the “occurrence” that caused it.

For the purposes of this insurance, electronic data is not tangible property.

As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from, computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

(Policies, p. 35; 2009 Policy, p. 32).

The following exclusions apply to the coverage provided under the Policy for property damage liability:

#### 2. Exclusions

This insurance does not apply to:

##### a. Expected or Intended Injury

“Bodily injury” or “property damage” expected or intended from the standpoint of the insured. This exclusion does not apply to “bodily injury” resulting from the use of reasonable force to protect persons or property.

##### b. Contractual Liability

“Bodily injury” or “property damage” for which the insured is obligated to pay damages by reason of the assumption of liability in a contract or agreement. This exclusion does not apply to liability for damages:

(1) That the insured would have in the absence of the contract or agreement; or

(2) Assumed in a contract or agreement that is an “insured contract”, provided the “bodily injury” or “property damage” occurs subsequent to the execution of the contract or agreement. Solely for the purposes of liability assumed in an “insured contract”, reasonable attorney fees and necessary litigation expenses incurred by or for a party other than an insured are deemed to be damages because of “bodily injury” or “property damage”, provided:

(a) Liability to such party for, or for the cost of, that party’s defense has also been assumed in the same “insured contract”; and

(b) Such attorney fees and litigation expenses are for defense of that party against a civil or alternative dispute resolution proceeding in

which damages to which this insurance applies are alleged.

(Policies, p. 17; 2009 Policy, p. 17).

The Policy contains a separate grant of coverage for liability for “personal and advertising injury,” defined as follows:

25. “Personal and advertising injury” means injury, including consequential “bodily injury,” arising out of one or more of the following offenses:
  - a. False arrest, detention or imprisonment;
  - b. Malicious prosecution;
  - c. The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that person occupies, committed by or on behalf of its owner, landlord or lessor;
  - d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person’s or organization’s goods, products or services;
  - e. Oral or written publication, in any manner, of material that violates a person’s right of privacy;
  - f. The use of another’s advertising idea in your “advertisement”; or
  - g. Infringing upon another’s copyright, trade dress or slogan in your “advertisement”.

(Policies, p. 34; 2009 Policy, p. 32).

In addition, “advertisement” is defined as follows:

1. “Advertisement” means a notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purposes of attracting customers and supporters.

For purposes of this definition:

- a. Notices that are published include material placed on the Internet or

on similar electronic means of communication; and

- b. Regarding web-sites, only that part of a web-site that is about your goods, products or services for the purposes of attracting customers or supporters is considered an advertisement.

(Policies, p. 31; 2009 Policy, p. 32).

Finally, with respect to “personal and advertising injury,” the Policy specifies the following exclusions to coverage that apply:

## 2. Exclusions

This insurance does not apply to:

### a. Knowing violation of Rights of Another

“Personal and advertising injury” caused by or at the direction of the insured with the knowledge that the act would violate the rights of another and would inflict “personal and advertising injury.”

...

### d. Contractual Liability

“Personal and advertising injury” for which the insured has assumed liability in a contract or agreement. This exclusion does not apply to liability for damages that the insured would have in the absence of the contract or agreement.

### e. Breach of Contract

“Personal and advertising injury” arising out of a breach of contract, except an implied contract to use another’s advertising idea in your “advertisement.”

...

### h. Infringement of Copyrights, Patent, Trademark or Trade Secret

“Personal and advertising injury” arising out of the infringement of

copyright, patent, trademark, trade secret or other intellectual property rights.

...

**j. Unauthorized Use of Another's Name or Product**

"Personal and advertising injury" arising out of the unauthorized use of another's name or product in your email address, domain name or meta-tag, or any other similar tactics to mislead another's potential customers.

(Policies, pp. 21–22; 2009 Policy, pp. 20–21).

The Court now turns to the allegations of BGS's complaint to determine whether there is any allegation which potentially comes within the coverage provided by the Policy.

*C. Count I—Misappropriation of Trade Secrets*

Count I of BGS's second amended complaint, misappropriation of trade secrets, is based on BGS's allegations that Denninghoff and SSO improperly acquired, disclosed, and used confidential information from the backup of the BGS Database Backup,<sup>5</sup> including the names and email addresses of thousands of BGS's customers [5:10–cv–00390, DE # 73 at ¶¶ 65–74]. BGS further alleges that Denninghoff disclosed BGS's confidential information to SSO, and that SSO used this information, with full knowledge that the information had been obtained by Denninghoff through means that were both improper and that violated the terms of his Non-Compete Agreement with BGS [*Id.*].

[16–18] Liberty first argues that the alleged misappropriation of BGS's trade secrets (the customer database) cannot constitute property damage under the Pol-

icy, as the terms of the Policy limit "property damage" to tangible property that is physically damaged or suffers loss of use. SSO responds by construing BGS's claim as a claim relating to mass mailings sent out by SSO to BGS's customer emails using the "converted" BGS customer email lists. SSO then states, with no citation to any authority, that the customer email list is a tangible piece of property. However, this argument ignores the general definition of "tangible property." *Black's Law Dictionary* defines "tangible property" as "[p]roperty that has physical form and characteristics." *Black's Law Dictionary* (9th ed. 2009). It is significant that what BGS alleges was misappropriated were BGS's customer's email addresses obtained from an electronic backup copy of BGS's customer database. Because such "property" has no physical form or characteristics, it simply does not fall within the definition of "tangible property." Moreover, the terms of the Policy clearly and unequivocally exclude "electronic data," including information stored, created or used on computer software, from the definition of "tangible property." Information obtained from BGS's customer database falls squarely within this exclusion. "Where the terms of an insurance policy are clear and unambiguous, the policy will be enforced as written." *Kemper*, 82 S.W.3d at 873 (citations omitted). Because there are no allegations involving the misappropriation of "tangible property," the misappropriation of trade secrets claim against SSO and Denninghoff is not covered as a "property damage" claim under the Policy. Although Liberty puts forth several alternative arguments regarding why Count I is not covered as a claim for "property damage," because it is clear that the property allegedly misappropriated (the customer

5. Defined in the second amended complaint as a "backup of BGS's customer database dated September 4, 2009, containing names,

email addresses, and other data regarding 204,058 persons throughout the United States" [5:10–cv–00390, DE # 73 at ¶ 54].

database) does not constitute “tangible property,” both as that term is generally understood, and also as that term is used in the Policy, the Court need not address these additional arguments.

Liberty further argues that the alleged misappropriation of BGS’s trade secrets cannot constitute “personal and advertising injury” under the Policy because this claim does not fall within any of the categories of “personal and advertising injury” specified in the Policy. SSO argues that this claim constitutes “the use of another’s advertising idea in your advertisement,” which is covered under the Policy as “personal and advertising injury.” Liberty points out that the Policy defines “advertisement” as “a notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purposes of attracting customers and supporters.” According to Liberty, because BGS’s customer database is not a notice that is broadcast or published, it cannot be an “advertisement.” However, Liberty overlooks that BGS’s misappropriation claim not only alleges that SSO and Denninghoff improperly obtained information from BGS’s database, but that it also used this information to generate email “blasts” from SSO to BGS’s customers. These email “blasts” would appear to constitute a notice that is broadcast to a specific market segment about SSO’s goods, products or services for the purpose of attracting customers, and, accordingly, potentially fall within the Policy’s definition of an “advertisement.” Thus, BGS’s claim for misappropriation of trade secrets is potentially covered as a “personal or advertising injury” under the Policy.

[19] However, the Policy giveth and the Policy taketh away. Liberty argues that, even if BGS’s trade secret misappropriation claim does allege “personal or advertising” injury, coverage is precluded for

this claim by the exclusions for breach of contract. The Policy specifically provides that coverage is not provided for “‘personal and advertising injury’ arising out of a breach of contract, except an implied contract to use another’s advertising idea in your ‘advertisement’” (Policies, p. 20, 2009 Policy p. 20). Liberty relies on an unpublished Sixth Circuit opinion, *Capitol Specialty Ins. v. Industrial Electronics, LLC*, 407 Fed.Appx. 47 (6th Cir.2011). In *Capitol Specialty Ins.*, an employee (Osyka) of the insured (Indel) allegedly disclosed customer and pricing lists, as well as other proprietary information, belonging to Osyka’s prior employer (ICS) to his new employer, Indel. *Id.* at 48. This disclosure was allegedly in violation of non-disclosure and confidentiality provisions of Osyka’s employment contract with ICS. *Id.* ICS also claimed that Indel used this information to its advantage and to the detriment of ICS. *Id.* ICS sued Osyka and Indel in state court, claiming: (1) that Indel tortiously interfered with ICS’s business relationship with Osyka by intentionally and improperly using ICS’s trade secrets and proprietary information; (2) Osyka breached his contract with ICS by disclosing proprietary and trade secret information to Indel; and (3) that Osyka and Indel violated the Kentucky Uniform Trade Secrets Act. *Id.* Indel sought coverage under a commercial general liability policy issued by Capitol. *Id.* Capitol filed a declaratory judgment action in federal court, seeking a declaration that it had no duty to defend or indemnify Indel and Osyka in the underlying state court action. *Id.*

On its motion for summary judgment, Capitol argued that the allegations of the underlying state court action fell outside the Policy’s coverage for “personal and advertising injury,” the only possible basis for coverage. *Id.* at 48–49. Capitol further argued that, even if the allegations of ICS’s complaint did fall within the Policy,

coverage was excluded by various exclusions, including an exclusion for breach of contract. *Id.* Notably, the “breach of contract” exclusion in the policy at issue excluded coverage for “[p]ersonal and advertising injury” arising out of a breach of contract, except an implied contract to use another’s advertising idea in your ‘advertisement.’” *Id.* at 49. Thus, the language of the exclusion at issue in *Capitol Specialty Ins.* is identical to the “breach of contract” exclusion at issue in this case.

After noting that the phrase “arising out of” should be construed broadly under Kentucky law, the Sixth Circuit held that the exclusion applied, as ICS’s claims against both Osyka and Indel arose directly from Osyka’s breach of contract. *Id.* at 50–51. As the Court explained, “Indel’s use of ICS’s proprietary and trade secret information—the basis of both the tortious interference and the statutory claims—grew out of, or flowed from, Osyka’s dissemination of such information to Indel. Without Osyka’s breach, Indel would have no information.” *Id.* at 51. The fact that ICS sued only Osyka, and not Indel, for breach of contract was of no consequence, as the exclusion requires only that the injury arise out of “a breach of contract.” *Id.* (emphasis in original). The Court found that “[t]his condition would be satisfied whether Osyka, Indel, or some other party breached a contract, and even regardless of whether ICS actually pled a breach of contract claim, so long as the asserted claims arose out of the breach.” *Id.*

In this case, BGS’s complaint alleges that SSO improperly acquired BGS’s customer database through Denninghoff, who had secretly and improperly kept the BGS Database Backup and other backup copies of BGS’s customer database after leaving his employment with BGS [5:10–cv–390, DE # 73 at ¶¶ 69–70]. The complaint further alleges that Denninghoff’s disclosure

of this information to SSO violated the terms of his Non-Compete Agreement with BGS [*Id.* at ¶ 71]. Thus, just as in *Capitol Specialty Ins.*, according to the allegations of BGS’s complaint, SSO’s use of BGS’s proprietary and trade secret information—the basis of the misappropriation claim—grew out of, or flowed from, Denninghoff’s dissemination of such information to SSO. Without Denninghoff’s breach of his Non-Compete Agreement, SSO would have no information. Accordingly, the Court finds that, under the clear and unambiguous language of the breach of contract exclusion, there is no coverage under the “personal and advertising injury” provisions of the Policy for the trade secret misappropriation claim.

For all of these reasons, to the extent that Liberty’s motion for summary judgment seeks a declaration that there is no coverage for Count I, trade secret misappropriation, Liberty’s motion shall be granted.

D. *Count II, Trademark Infringement and Count III, Breach of Tradename License Agreement*

In Count II, BGS alleges trademark infringement in violation of 15 U.S.C. § 1125, the Lanham Act [5:10–cv–390, DE # 73]. Specifically, BGS alleges that, although SSO had a nonexclusive license to use the “Bud’s Gun Shop” mark and similar marks pursuant to the Tradename License Agreement between the parties, SSO’s breach of that agreement caused the License to immediately terminate [*Id.*]. BGS further alleges that, notwithstanding the termination of this License Agreement, SSO has knowingly continued to use the “Bud’s Gun Shop” trademark in a variety of ways to promote its business with its suppliers and the consuming public and that this use has damaged BGS by causing harm to BGS’s identity, reputation, and



goodwill and by causing actual confusion among buyers and sellers in the firearms market and more generally among the consuming public [*Id.*]. Similarly, in Count III, BGS brings a breach of contract claim against SSO for its breach of the Tradename License Agreement [*Id.*]. Specifically, BGS alleges that, despite the fact that, as early as July 2009, SSO's over-the-counter sales of firearms from its retail store comprised less than 85% of its total sales of firearms during multiple calendar month periods, SSO continued to use the Bud's tradename, all in material breach of the Tradename License Agreement [*Id.*].

[20] Liberty argues that the claim for trademark infringement cannot constitute property damage under the Policy, as the terms of the Policy limit "property damage" to coverage for tangible property that is physically damaged or suffers loss of use. Liberty similarly argues that the breach of contract claim in Count III does not allege property damage. In response, SSO argues that the damages claimed by BGS—including the harm to BGS's identity, reputation and goodwill—are property damages. However, SSO completely overlooks that the question is not whether BGS seeks property damages. Rather, under the terms of the Policy, there is only coverage if BGS claims damage to *tangible* property that is physically damaged or suffers loss of use. Neither identity, reputation nor goodwill constitutes property that has "physical form and characteristics," and, therefore, none is tangible property. *Blacks Law Dictionary* (9th ed. 2009). Indeed, identity, reputation and goodwill are quintessential examples of *intangible* property.

6. SSO's reliance on BGS's allegations regarding SSO's unauthorized email blast advertisement resulting from the alleged theft of BGS's customer database in support of its argument that coverage should be found for Counts II and III of BGS's complaint is curious, given

SSO also responds that the Policy's coverage for "loss of use of tangible property," "by its plain language, would include BGS's loss of the use of the 'Bud's' name for its products, after SSO allegedly breached the license agreement" [DE # 38 at p. 8]. However, SSO cites to no authority holding that the loss of a mark constitutes the loss of *tangible* property. More importantly, SSO overlooks that there are no allegations that BGS has lost the use of the "Bud's" name for its products. In fact, BGS's complaint alleges the complete opposite—it alleges that BGS continues to use, promote and advertise the Bud's Gun Shop Marks for its goods and services and that SSO's continued use of the "Bud's Gun Shop" name, allegedly in violation of the License, has caused confusion in the marketplace [5:10-cv-390, DE # 73 at Count II].

Finally, SSO argues that "[p]resumably one of the damages asserted by BGS as a result of SSO's unauthorized email blast advertisement would be its inability to sell those goods that were lost to SSO by virtue of the advertisements" [DE # 38 at p. 10].<sup>6</sup> SSO then claims that "[v]arious courts have held this to be a property damage as defined as 'loss of use of tangible property that is not physically injured,'" citing *Lucker Mfg. Inc. v. Home Ins. Co.*, 23 F.3d 808, 816-817 (3d Cir.1994) [*Id.*]. However, SSO grossly misrepresents the Court's holding in *Lucker*. In *Lucker*, the Court analyzed whether, in a Comprehensive General Liability Insurance ("CGL") policy, "the clause 'loss of use of tangible property that has not been physically injured' covered costs of preventing a defective component from becoming incor-

that Counts II and III relate solely to SSO's alleged breach of the Trademark License Agreement. BGS does not mention the alleged theft of the customer database or SSO's email blasts in Count II or Count III.

porated into a product that has been designed but has not yet been manufactured.” *Id.* at 810. The Court separated the inquiry into two parts: (1) whether a change in demand for a product in the marketplace brought about by the insured’s wrongful act constitutes a “loss of use”; and (2) whether a design for a product is “tangible property.” *Id.* at 811. The quote selectively cited by SSO—“the loss of a non-physical use of a product, such as offering it for sale, should be considered a “loss of use”; and that the decreased value of a product because of loss of customer acceptance of the product is a “loss of use” within the meaning of the standard CGL policy”—appears in the portion of the Court’s opinion discussing whether a change in demand for a product is a loss of use. *Id.* at 814–818. SSO then stretches this quote to suggest that *Lucker* held that such “loss of use” property damage is necessarily the “loss of use of *tangible* property,” ignoring that the word “tangible” does not appear once in this entire section of the Court’s opinion. *Id.* In fact, the Court in *Lucker* held that, in that case, even though there was “loss of use” damage, the property that was allegedly damaged was *not* tangible property, therefore there was no coverage under the CGL policy at issue. *Id.* at 818. Incredibly, SSO also overlooks that the *Lucker* Court points to goodwill, reputation, profits, trademarks and trade secrets—the “property” allegedly damaged in this case—as examples of *intangible* property. *Id.* at 819. Suffice it to say, SSO’s reliance on *Lucker* is misplaced.

For all of these reasons, the Court finds that neither Count II nor Count III of BGS’s complaint allege “property damage” under the terms of the Policy. Therefore, the Court finds that there is no coverage for either the trademark infringement claim (Count II) or the breach of contract claim (Count III) under the “property damage” provisions of the Policy.

[21] Liberty further argues that there is no coverage for Count II under the “personal and advertising injury” provisions of the Policy, as the clear and unambiguous language of the Policy states that “[t]his insurance does not apply to . . . ‘personal and advertising injury’ arising out of the infringement of copyright, patent, trademark, trade secret or other intellectual property rights” [Policies, pp. 21; 2009 Policy, pp. 20–21]. According to Liberty, because Count II solely and specifically alleges that SSO improperly utilized BGS’s marks, there is no coverage under the Policy for this claim. Moreover, Liberty argues that there is no coverage for the Count III breach of contract claim under the “personal and advertising injury” provisions of the Policy, as this claim does not allege “personal and advertising injury” as defined by the Policy.

[22] SSO responds that the Policy provides coverage for “personal and advertising injury” arising out of oral or written publication, in any manner, of material that disparages a person’s or organization’s goods or services. Because Counts II and III of BGS’s complaint allege that SSO’s use of the “Bud’s Gun Shop” mark caused harm to—or disparaged—BGS’s identity, reputation and good will, SSO argues that these allegations come within the coverage provided under “personal and advertising injury” for disparagement. However, this argument ignores the clear and unambiguous language of the Policy precluding coverage for a claim arising out of the infringement of trademark or other intellectual property rights. Kentucky law is clear exclusions that are “unequivocally conspicuous, plain and clear” will be enforced. *Kentucky Ass’n of Counties All Lines Fund Trust*, 157 S.W.3d at 634. Notwithstanding BGS’s allegation that SSO’s use of BGS’s mark “disparaged” BGS’s good will, BGS’s claim in Count II is

still a claim for trademark infringement, the very claim for which the Policy explicitly precludes coverage.

[23, 24] SSO also attempts to characterize BGS's claim that SSO's use of the tradename "Bud" and "Bud's Gun Shop" in violation of the Lanham act as a claim "under 'trade dress' or 'copyright' or 'slogan'" rather than a claim involving a trademark. Although it is not clear, presumably, by attempting to characterize BGS's claim as a "trade dress" or copyright claim, SSO is attempting to get around the exclusion for trademark infringement claims. However, "[t]rademarks and trade dress are separate and distinct causes of action under the Lanham Act." *General Motors Corp. v. Lanard Toys, Inc.*, 468 F.3d 405, 414 (6th Cir.2006) (citations omitted). In *Gibson Guitar Corp. v. Paul Reed Smith Guitars, LP*, 423 F.3d 539, 547 (6th Cir.2005), the Sixth Circuit explained that "[t]he Lanham Act defines a trademark as 'any word, name, symbol, or device, or any combination thereof' which is used or intended to be used by a person 'in commerce ... to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown.'" *Id.* (quoting 15 U.S.C. § 1127). However, "[b]y contrast, trade dress is not explicitly defined in the Lanham Act, but has been described by the Supreme Court as the 'design or packaging of a product' which has acquired a 'secondary meaning' sufficient 'to identify the product with its manufacturer or source.'" *Id.* (quoting *TrafFix Devices, Inc. v. Mktg. Displays, Inc.*, 532 U.S. 23, 28, 121 S.Ct. 1255, 149 L.Ed.2d 164 (2001)). Count II of BGS's complaint clearly alleges that SSO continued to use various BGS marks, despite the expiration of the Tradename License, in violation of the Lanham Act. There are no allegations regarding the design or packaging of a product, or

any other similar allegations regarding the image of a product, that would suggest that BGS's claim was actually a trade dress claim.

SSO also attempts to create an ambiguity by arguing that it is confusing for the Policy to include "[i]nfringing upon another's copyright, trade dress or slogan in your 'advertisement'" within the definition of "personal and advertising injury," while subsequently excluding coverage for "'personal and advertising injury' arising out of the infringement of copyright, patent, trademark, trade secret or other intellectual property rights." According to SSO, because the average man would not know the difference between trademark and trade dress, the Court should strike this exclusion and find coverage and/or a duty to defend.

[25, 26] It is true that, in Kentucky, under the reasonable expectations doctrine, ambiguous terms in an insurance contract must be interpreted in favor of the insured's reasonable expectations and construed as an average person would construe them. But, "[o]nly actual ambiguities, not fanciful ones, will trigger application of the doctrine." *True v. Raines*, 99 S.W.3d 439, 443 (Ky.2003). Indeed, "[a] non-existent ambiguity [should not] be utilized to resolve a policy against an insurer. It is not enough for one party to claim ambiguity. The mere fact that [a party] attempt[s] to muddy the water and create some question of interpretation does not necessarily create an ambiguity." *Kentucky Ass'n of Counties All Lines Fund Trust*, 157 S.W.3d at 633-634 (citations omitted) (alterations in original). Exclusions that are "unequivocally conspicuous, plain and clear" will be enforced. *Id.* at 634.

[27] Under Kentucky law, "[a] contract is ambiguous if a reasonable person would find it susceptible to different or inconsis-

tent interpretations.” *Wehr Constructors, Inc. v. Assurance Co. of America*, 384 S.W.3d 680, 687 (Ky.2012) (quoting *Hazard Coal Corp. v. Knight*, 325 S.W.3d 290, 298 (Ky.2010)). Here, there is nothing ambiguous about the Policy’s exclusion of coverage for claims of trademark infringement. Indeed, it would be patently unreasonable for a person to believe that the clear language of the Policy excluding coverage for personal and advertising injury “arising out of the infringement of . . . trademark, trade secret or other intellectual property rights” means anything other than such claims are excluded from coverage. Because the language of the Policy is unambiguous, the “reasonable expectations” doctrine is inapplicable. Accordingly, the Court finds that the exclusion of coverage for “personal and advertising injury” arising out of trademark infringement applies, thus precluding coverage for Count II of BGS’s complaint.

SSO does not point the Court to any other category of “personal and advertising injury” as defined by the Policy that would purportedly include coverage for the Count III breach of contract claim. Indeed, BGS’s breach of the Trademark License Agreement claim does not allege injury arising out of false arrest, detention or imprisonment; malicious prosecution; wrongful eviction from or wrongful entry into property; or oral or written publication of material violating a person’s right of privacy. Thus, there are no grounds for finding that Count III is covered as “personal and advertising injury.” Accordingly, the Court finds that BGS’s claim for breach of contract in Count III does not allege “personal and advertising injury.” Thus, there is no coverage for this claim under the Policy.

In the alternative, Liberty argues that, even if “personal and advertising injury” were alleged, coverage for Counts II and III is also excluded under the Policy’s

exclusion of coverage for “‘personal and advertising injury’ arising out of a breach of contract, except an implied contract to use another’s advertising idea in your ‘advertisement’” [Policies p. 21; 2009 Policy p. 21]. According to Liberty, because the trademark infringement claim arises solely because SSO allegedly failed to comply with the License Agreement between the parties, which otherwise authorized SSO’s use of the marks, the breach of contract exclusion also applies to bar coverage for the claim. Liberty relies on the allegations of BGS’s complaint, which specify that Count II arises only and directly from SSO’s alleged breach of the License Agreement between the parties, as well as the broad interpretation of the phrase “arising under” applied by the Sixth Circuit in *Capitol Specialty Ins.*, 407 Fed. Appx. at 51, discussed above. Similarly, because Count III is a claim for breach of contract, there can be no doubt that Count III arises out of a breach of contract claim.

[28] SSO does not respond to Liberty’s argument that the exclusion for personal and advertising injury arising from breach of contract bars coverage for Count II’s trademark infringement claim or for Count III’s breach of contract claim, thus waiving the opportunity. *Guarino v. Brookfield Tp. Trustees*, 980 F.2d 399, 405 (6th Cir. 1992) (on a motion for summary judgment, the non-moving party’s burden to respond by showing that there is a genuine issue for trial “is really an opportunity to assist the court in understanding the facts. But if the non-moving party fails to discharge that burden—for example, by remaining silent—its opportunity is waived and its case is wagered.”). This reason alone is sufficient to find in Liberty’s favor with respect to these claims. Even so, under Kentucky law, “each exclusion is to be read independently of every other exclusion.” *Kemper*, 82 S.W.3d at 874 (citations

omitted). As explained in *Kemper*, “Because an exclusion is not an affirmative grant of coverage—and each exclusion is independent of all others—any applicable exclusion is sufficient to remove coverage. In other words, ‘[i]f any one exclusion applies there should be no coverage, regardless of inferences that might be argued on the basis of exceptions or qualifications contained in other exclusions.’” *Id.* at 874 (quoting *Weedo v. Stone-E-Brick, Inc.*, 81 N.J. 233, 405 A.2d 788, 790 (1979), quoting *Tinker*, “Comprehensive General Liability Insurance—Perspective and Overview” 25 *Feder. Ins. Coun. Q.* 217, 223 (1975)). Here, the Court finds that, because BGS’s claim arises directly from SSO’s alleged breach of the Tradename License Agreement, even if the trademark infringement exclusion did not apply, the breach of contract exclusion independently precludes coverage for Count II of BGS’s complaint. Similarly, because there can be no question that Count III’s breach of the Tradename License Agreement arises out of a breach of contract claim, the breach of contract exclusion also precludes coverage for that claim. Accordingly, the Court finds that Liberty is entitled to summary judgment with respect to coverage for Count II, the trademark infringement claim, and Count III, the breach of contract claim.

E. *Remaining Counts of BGS’s Second Amended Complaint*

The remaining counts of BGS’s second amended complaint are as follows: Count IV—breach of fiduciary duty (against Denninghoff); Count V—aiding and abetting breach of fiduciary duty (against SSO); Count VI—breach of contract—non-compete agreement (against Denninghoff); Count VII—tortious interference with contract (against SSO); Count VIII—violation of 18 U.S.C. § 1030(a)(2) (the “Computer Fraud and Abuse Act”); Count IX—violation of 18 U.S.C. § 1030(a)(4); Count X—

violation of K.R.S. § 434.845 (unlawful access of computer); and Count XI—violation of K.R.S. § 434.855 (misuse of computer information) [5:10-cv-390, DE # 73]. The complaint also seeks injunctive relief and exemplary and/or punitive damages [*Id.*]. Liberty argues that coverage is precluded for each of these claims for various reasons, including that these claims do not allege property damage or personal and advertising injury and that, even if they did, coverage is precluded by various specific exclusions. SSO has chosen not to respond to any of these arguments. For this reason alone, summary judgment in Liberty’s favor may be appropriate. *Guarino*, 980 F.2d at 405 (6th Cir.1992).

Regardless of SSO’s failure to respond, the Court has reviewed the terms of the Policy and the allegations of BGS’s complaint and agrees with Liberty’s arguments that none of the above counts allege property damage. Rather, these claims all relate to the alleged improper procurement, disclosure and use of confidential information and data on BGS’s computer network system. As discussed above, information on BGS’s computer system, including its customer database, is not tangible property, thus these claims do not allege property damage.

With respect to the Policy’s coverage for “personal and advertising injury,” there are no allegations of injury arising out of false arrest, detention or imprisonment; malicious prosecution; wrongful eviction from or wrongful entry into property; oral or written publication of material violating a person’s right of privacy; or infringing upon another’s copyright, trade dress or slogan in an advertisement. As discussed above, to the extent that these claims allege that SSO and Denninghoff used the improperly acquired information to generate email blasts to customers, these claims could potentially be considered to allege

“personal and advertising injury” arising from the use of another’s advertising idea in an advertisement. However, even if these allegations potentially alleged “personal and advertising injury,” these claims all arise from the allegations of Denninghoff’s improper access and disclosure of BGS’s confidential information, in breach of his non-compete agreement with BGS. Thus, these claims arise out of breach of contract and, accordingly, coverage is precluded by the breach of contract exclusions contained in the Policy. *Capitol Specialty Ins.*, 407 Fed.Appx. at 51.

For all of these reasons, the Court finds that the Policy does not provide coverage for any of the remaining counts of BGS’s second amended complaint. Accordingly, Liberty is entitled to summary judgment.

#### F. *Remainder of Liberty’s Motion*

Liberty seeks a declaration that no coverage is provided for BGS’s claim for injunctive relief, as language in the Policy that limits the applicability of the Policy to claims for liability and does not include equitable relief (Policies, p. 16; 2009 Policy, p. 16; Policies, p. 21; 2009 Policy, p. 20). However, because the Court finds that the Policy does not provide coverage for any of the damages alleged by BGS, it is unnecessary to decide whether, even if the Policy provided coverage, this coverage would be for liability only and would not extend to any equitable relief. Similarly, the Court need not consider Liberty’s request for a declaration that the Policy does not provide coverage for any claims for exemplary or punitive damages. In addition, because the Court has found that there is no coverage for any of the claims made against Denninghoff, it is unnecessary for the Court to determine whether he is an “insured” under the Policy.

#### IV. CONCLUSION

For the reasons set forth above, the Court finds the Policy does not provide coverage to SSO and/or Denninghoff for the claims made against them in the underlying litigation. Accordingly, Liberty has no duty to defend or indemnify SSO and/or Denninghoff with respect to these claims. Thus, Liberty’s motion for summary judgment shall be granted.

For all of the foregoing reasons, the Court, being fully and sufficiently advised, **HEREBY ORDERS** that:

- (1) The Policy at issue does not provide coverage to Defendants Security Safe Outlet, Inc., d/b/a Bud’s Gun Shop and/or Matthew Denninghoff for the claims made against them in the underlying litigation, *Budsgunshop.com, LLC v. Security Safe Outlet, Inc., et al.*, Case # 5:10-cv-390, pending in the United States District Court, Eastern District of Kentucky;
- (2) Liberty is not obligated or required to defend or indemnify SSO or Denninghoff with respect to the claims made against them in the underlying litigation;
- (3) Liberty has no other obligation or duty to either Budsgunshop.com, Marion E. Wells, Jr., Rex McClanahan, or any other party, arising out of the claims made in the underlying litigation;
- (4) Liberty’s motion for summary judgment [DE # 37] is **GRANTED**;
- (5) Liberty’s request for oral argument is **DENIED**;
- (6) All matters having been resolved in this case, judgment in favor of Plaintiff shall be entered contemporaneously with this Opinion & Order pursuant to Fed. R. Civ. Pro. 58; and

- (7) this matter is **STRICKEN** from the active docket.



**IRSHAD LEARNING CENTER,**  
**Plaintiff,**  
 v.  
**COUNTY OF DUPAGE, Defendant.**  
**No. 10 CV 2168.**

United States District Court,  
 N.D. Illinois,  
 Eastern Division.

March 29, 2013.

**Background:** Muslim religious and educational group brought action against county zoning board of appeals (ZBA) and county board, alleging that denial of conditional use permit to use property for religious services and educational purposes violated group's rights under Religious Land Use and Institutionalized Persons Act (RLUIPA), First and Fourteenth Amendments, and Illinois law. Both sides moved for summary judgment.

**Holdings:** The District Court, Rebecca R. Pallmeyer, J., held that:

- (1) secular private school formerly operating on land was not an appropriate comparator for purposes of as-applied equal-terms challenge under RLUIPA;
- (2) Korean church was not identical or directly comparable in all relevant respects to plaintiff, as required to support claim for violation of Equal Protection Clause;
- (3) there was no evidence board denied permit because of plaintiff's religion;
- (4) board's denial substantially burdened plaintiff's religious exercise, within the meaning of both RLUIPA and Illinois Religious Freedom Restoration Act (RFRA); and

- (5) denial of special use permit did not comply with applicable zoning criteria, and thus, was arbitrary as a matter of substantive due process.

Ordered accordingly.

### 1. Civil Rights ⇐1073

To prevail on an equal-terms claim under RLUIPA, which prohibits a government body from imposing or implementing a land use regulation in a manner that treats a religious assembly or institution on less than equal terms with a nonreligious assembly or institution, movant must show that religious and secular land uses have not been treated the same from the standpoint of an accepted zoning criterion. Religious Land Use and Institutionalized Persons Act of 2000, § 2(b)(1), 42 U.S.C.A. § 2000cc(b)(1).

### 2. Civil Rights ⇐1073

A plaintiff bringing an as-applied equal-terms challenge under RLUIPA must present evidence that a nonreligious comparator received unequal treatment under the challenged regulation. Religious Land Use and Institutionalized Persons Act of 2000, §§ 2(b)(1), 4(b), 42 U.S.C.A. §§ 2000cc(b)(1), 2000cc-2(b).

### 3. Civil Rights ⇐1073

RLUIPA does more than require that land use regulations contain equal terms for religious and non-religious uses; it requires that government treat religious assemblies or institutions on equal terms. Religious Land Use and Institutionalized Persons Act of 2000, § 2(b)(1), 42 U.S.C.A. § 2000cc(b)(1).

### 4. Civil Rights ⇐1073

RLUIPA equal-terms provision is violated when a religious use is not permitted, but a secular use is, only where the two uses do not differ with respect to any accepted zoning criterion. Religious Land

147 Conn.App. 450

**RECALL TOTAL INFORMATION  
MANAGEMENT, INC., et al.**

v.

**FEDERAL INSURANCE  
COMPANY et al.****No. 34716.**

Appellate Court of Connecticut.

Argued Oct. 11, 2013.

Decided Jan. 14, 2014.

**Background:** Insureds, a records storage company and its transportation subcontractor, brought action against commercial general liability (CGL) insurers for breach of insurance contract and other claims, arising from denial of coverage for insureds' negotiated settlement with client for reimbursement of more than \$6 million in client's expenses associated with mitigating the losses caused when insureds lost client's data tapes containing employees' personal data during transport. The Superior Court, Judicial District of Hartford, Berger, J., 2012 WL 469988, granted summary judgment in favor of insurers on the breach of insurance contract claim, and denied insureds' motion for reargument. Insureds appealed.

**Holdings:** The Appellate Court, Lavine, J., held that:

- (1) settlement negotiations with client that resulted in reimbursement of client's costs did not constitute "suit" or "other dispute resolution proceeding," which liability insurers had duty to defend under CGL policy;
- (2) loss of client's data storage tapes was not covered under CGL policy's personal injury provision; and
- (3) triggering of statutes that required notification of affected persons when there was an invasion of privacy did

not constitute presumptive invasions of privacy under CGL policy.

Affirmed.

**1. Judgment ⇨185(6)**

On a motion for summary judgment, the judgment sought shall be rendered forthwith if the pleadings, affidavits and any other proof submitted show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.

**2. Judgment ⇨181(2)**

A "material fact," in deciding a motion for summary judgment, is a fact that will make a difference in the result of the case.

See publication Words and Phrases for other judicial constructions and definitions.

**3. Judgment ⇨183**

The facts at issue, in deciding a motion for summary judgment, are those alleged in the pleadings.

**4. Judgment ⇨185(2)**

The party seeking summary judgment has the burden of showing the absence of any genuine issue as to all material facts, which, under applicable principles of substantive law, entitle him to a judgment as a matter of law.

**5. Judgment ⇨185(2)**

The party adverse to a motion for summary judgment must provide an evidentiary foundation to demonstrate the existence of a genuine issue of material fact.

**6. Judgment ⇨185(2)**

In deciding a motion for summary judgment, the trial court must view the evidence in the light most favorable to the nonmoving party.



**7. Judgment ⇨185(6)**

The test, in deciding a motion for summary judgment, is whether a party would be entitled to a directed verdict on the same facts.

**8. Judgment ⇨185(5)**

While the court must view the inferences to be drawn from the facts in the light most favorable to the party opposing a motion for summary judgment, a party may not rely on mere speculation or conjecture as to the true nature of the facts to overcome a motion for summary judgment.

**9. Appeal and Error ⇨901**

On appeal, the burden is on the opposing party to demonstrate that the trial court's decision to grant the movant's summary judgment was clearly erroneous.

**10. Appeal and Error ⇨863**

The appellate court's review of the trial court's decision to grant a motion for summary judgment is plenary.

**11. Appeal and Error ⇨893(1)**

Construction of a contract of insurance presents a question of law for the trial court which the appellate court reviews de novo.

**12. Insurance ⇨2918, 3111(3)**

Two years of settlement negotiations with client and between insureds, that resulted in \$6 million settlement for reimbursement of client's costs for mitigating loss of computer data tapes that contained employees' personal information, did not constitute "suit" or "other dispute resolution proceeding," which liability insurers had duty to defend under commercial general liability (CGL) policy, and thus insurers did not waive coverage defenses by failing to defend; insureds failed to cite any authority supporting interpretation that negotiations following a demand fit within definition of those terms, and such

an interpretation would create an internal inconsistency within the policy as it would merge the term "claim" with "suit," as insured was obligated to provide notice of both, but insurer only had duty to defend "suits."

See publication Words and Phrases for other judicial constructions and definitions.

**13. Insurance ⇨2290, 2939**

Where an insured alleges that an insurer has improperly failed to defend and provide coverage for underlying claims that the insured has settled, the insured has the burden of proving that the claims were within the policy's coverage.

**14. Insurance ⇨1806**

An insurance policy is to be interpreted by the same general rules that govern the construction of any written contract.

**15. Insurance ⇨1813, 2090**

In accordance with the principles governing construction of any written contract, the determinative question when interpreting an insurance policy is the intent of the parties, that is, what coverage the insured expected to receive and what the insurer was to provide, as disclosed by the provisions of the policy.

**16. Insurance ⇨1809, 1822**

If the terms of the insurance policy are clear and unambiguous, then the language, from which the intention of the parties is to be deduced, must be accorded its natural and ordinary meaning; under those circumstances, the policy is to be given effect according to its terms.

**17. Insurance ⇨1810, 1816**

When interpreting an insurance policy, courts must look at the contract as a whole, consider all relevant portions together and, if possible, give operative effect to every provision in order to reach a reasonable overall result.

**18. Insurance** ⇨1808, 1827

In determining whether the terms of an insurance policy are clear and unambiguous, a court will not torture words to import ambiguity where the ordinary meaning leaves no room for ambiguity.

**19. Contracts** ⇨143(2)

Any ambiguity in a contract must emanate from the language used in the contract rather than from one party's subjective perception of the terms.

**20. Insurance** ⇨1808

As with contracts generally, a provision in an insurance policy is ambiguous when it is reasonably susceptible to more than one reading.

**21. Insurance** ⇨1832(2), 1833

Any ambiguity in the terms of an insurance policy must be construed in favor of the insured because the insurance company drafted the policy; this rule of construction may not be applied, however, unless the policy terms are indeed ambiguous.

**22. Insurance** ⇨1810, 1814

A construction of an insurance policy which entirely neutralizes one provision should not be adopted if the contract is susceptible of another construction which gives effect to all of its provisions and is consistent with the general intent.

**23. Insurance** ⇨2918

Even if phrase "other dispute resolution proceeding," in commercial general liability (CGL) policy, included settlement negotiations that lasted for two years between insured records storage company and records transportation subcontractor, and the client whose data tapes they lost, that alone would not trigger the liability insurers' duty to defend; CGL policy required that insurers consent to the proceeding, insurers did not consent to the

negotiations, and thus the duty to defend was not triggered.

**24. Insurance** ⇨2312

Conduct of insureds, a records storage company and its transportation subcontractor, in losing client's data storage tapes containing employees' personal data did not result in "publication" of material that violated person's right to privacy and, thus, did not result in a "personal injury" covered by commercial general liability (CGL) policy; there was no evidence that personal information on the tapes was actually accessed by whoever took the tapes, and no employees had suffered injury as a result of the tapes being lost.

See publication Words and Phrases for other judicial constructions and definitions.

**25. Insurance** ⇨2312

Regardless of the precise definition of "publication," within meaning of commercial general liability (CGL) policy's personal injury provision, which covers publication of material that violated a person's right to privacy, access is a necessary prerequisite to the communication or disclosure of personal information.

**26. Insurance** ⇨2312

Fact that notification statutes were triggered by insured records storage company's and transportation subcontractor's loss of client's confidential employee data tapes, that required notification of affected persons when there was an invasion of privacy, did not constitute presumptive invasions of privacy, and thus "personal injury," within meaning of commercial general liability (CGL) policy that defined covered personal injury to include publication of material that violated a person's right to privacy; notification statutes did not address or otherwise provide for compensation from identity theft or the increased risk thereof, and statutes merely required

notification to an affected person so that he may protect himself from potential harm, which was not a substitute for a personal injury. C.G.S.A. § 36a-701b; N.Y.McKinney's General Business Law § 899-aa(2).

---

Edmund M. Kneisel, pro hac vice, with whom were Lawrence G. Rosenthal, and, on the brief, Matthew T. Wax-Krell, Hartford, and Brian K. Epps, pro hac vice, for the appellants (plaintiffs).

Melicent B. Thompson, with whom was Eric S. Lankton, Simsbury, for the appellee (named defendant).

Robert D. Laurie, with whom, on the brief, was Elizabeth F. Ahlstrand, for the appellee (defendant Scottsdale Insurance Company).

LAVINE, KELLER and SULLIVAN,  
Js.

LAVINE, J.

<sup>1</sup><sub>452</sub>This breach of an insurance contract dispute involves the interpretation of a personal injury clause in a commercial general liability policy. The plaintiffs, Recall Total Information Management, Inc. (Recall) and Executive Logistics, Inc. (Ex Log), appeal from the grant of summary judgment in favor of the defendants, Federal Insurance Company (Federal) and <sup>1</sup><sub>453</sub>Scottsdale Insurance Company (Scottsdale).<sup>1</sup> On appeal, the plaintiffs claim that the trial court improperly construed the

insurance contract at issue by concluding that (1) the defendants did not have a duty to defend, and (2) the losses associated with a data-loss incident were not personal injuries. We affirm the judgment of the trial court.

The following facts, as agreed to in the parties' stipulation of facts, are germane to the resolution of this appeal. In October, 2003, Recall entered into a vital records storage agreement with International Business Machines (IBM) whereby Recall agreed to transport and store various electronic media belonging to IBM. In February, 2006, Recall entered into a subcontract with Ex Log to provide transportation services for the electronic media. Under the subcontract with Recall, Ex Log was required to maintain various insurance policies, including a \$2 million commercial general liability policy and a \$5 million umbrella liability policy, all naming Recall as an additional insured. The defendants issued the required insurance.<sup>2</sup>

On February 23, 2007, Ex Log dispatched a transport van to move computer tapes (tapes) from an IBM facility in New York to another location. During transport, a cart containing the tapes fell out of the back of the van near a highway exit ramp. The parties agree that approximately 130 of the tapes were removed from the roadside by an unknown person and never recovered.

<sup>1</sup><sub>454</sub>The tapes that were never recovered contained employment-related data for some 500,000 past and present IBM employees. This information included social

1. Sinclair Risk and Financial Services, LLP, was a defendant before the trial court but is not a party to this appeal.
2. Federal issued a commercial general liability policy containing a per occurrence limit of \$1 million and an aggregate limit of \$2 million. Scottsdale issued a commercial liability

umbrella policy containing a per occurrence limit of \$4 million. Although these are two separate policies, the relevant provisions are nearly identical. For the purposes of this opinion, we use the term "policy" in the singular and quote the language from the policy issued by Federal.

security numbers, birthdates, and contact information. After being notified that the tapes had been lost, IBM immediately took steps to prevent harm from any dissemination of this personal information. These steps included notification to potentially affected employees and the establishment of a call center to answer inquiries regarding the lost data. IBM also provided those who could be affected by the loss with one year of credit monitoring to protect against identity theft. IBM claimed a total of more than \$6 million in expenses<sup>3</sup> for the mitigation measures it took and entered into a negotiated settlement with Recall for the full amount of the loss.

Thereafter, Recall sought indemnification from Ex Log. Ex Log then filed claims against the policy, but the defendants denied coverage. Following the denial of coverage, Recall and Ex Log entered into a settlement agreement and on June 22, 2009, Ex Log signed a promissory note in favor of Recall for \$6,419,409.79 and assigned all of its rights under the policy to Recall.

The plaintiffs commenced the present action against the defendants on July 24, 2009. The complaint alleged several counts, including breach of an insurance contract. The defendants filed motions for summary judgment with respect to the count alleging breach of an insurance contract on the ground that, as a matter of law, they had no duty to defend and that the plaintiffs' loss was not covered by the policy. The trial court granted the motions for summary judgment, concluding

that the defendants had not waived their coverage<sup>4</sup> defenses and that the plaintiffs' losses were not covered under either the property damage or the personal injury provisions of the policy.

With respect to whether the defendants had waived their coverage defenses, the trial court concluded that, under the policy, the defendants only had a duty to defend against a "suit." The trial court found that the term "suit" was unambiguous and declined to interpret that term to include mere negotiations. The trial court then turned to whether the loss associated with the lost tapes was covered under the terms of the policy. The trial court addressed whether the loss was covered under the property damage provision of the policy and determined that the data loss constituted intangible property, which was expressly excluded from coverage.<sup>4</sup>

Next, the trial court addressed whether there was coverage under the personal injury provision of the policy. The trial court noted that the plaintiffs did not allege that the information contained on the tapes was ever accessed by anyone following the incident in which the tapes were lost. Accordingly, the trial court reasoned: "[T]here has also been no injury to a person. IBM paid notification costs, but IBM is not a person<sup>5</sup> and there is no allegation that its right to privacy was violated. Additionally, there is no evidence—even now, some four years after the incident—that any person suffered identity theft or that the privacy of any IBM employee was violated as a result of

3. In addition to providing credit monitoring to the affected employees, IBM provided credit restoration to some of its employees. The parties agree that no identity theft incident could be traced to the loss of the IBM tapes, however.

4. This determination is not challenged on appeal.

5. We interpret the court's statement to mean that IBM is not a person for the purposes of privacy law. See 3 Restatement (Second), Torts, Invasion of Privacy § 652I, comment (c), p. 403 (1977) ("[a] corporation, partnership or unincorporated association has no personal right to privacy").

the loss or theft of the data tapes.” The trial court then rendered summary judgment in favor of the defendants. The plaintiffs filed <sup>1456</sup>a motion for reargument, which was denied. This appeal followed.<sup>6</sup>

On appeal, the plaintiffs contend that the trial court erred when it construed the policy and concluded that (1) the defendants did not have a duty to defend, and (2) the loss of the tapes did not constitute a personal injury. We disagree.

[1–7] “Our standard of review of a trial court’s decision to grant a motion for summary judgment is well established. . . . The judgment sought shall be rendered forthwith if the pleadings, affidavits and any other proof submitted show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. . . . A material fact is a fact that will make a difference in the result of the case. . . . The facts at issue are those alleged in the pleadings. . . . The party seeking summary judgment has the burden of showing the absence of any genuine issue as to all material facts, which, under applicable principles of substantive law, entitle him to a judgment as a matter of law. . . . [T]he party adverse to such a motion must provide an evidentiary foundation to demonstrate the existence of a genuine issue of material fact. In deciding a motion for summary judgment, the trial court must view the evidence in the light most favorable to the nonmoving party. . . . The test is whether a party would be entitled to a directed verdict on the same facts. . . .

[8–11] “While the court must view the inferences to be drawn from the facts in the light most favorable to the party op-

posing the motion . . . a party may not rely <sup>1457</sup>on mere speculation or conjecture as to the true nature of the facts to overcome a motion for summary judgment. . . . On appeal, however, the burden is on the opposing party to demonstrate that the trial court’s decision to grant the movant’s summary judgment was clearly erroneous.” (Citations omitted; internal quotation marks omitted.) *Norse Systems, Inc. v. Tingley Systems, Inc.*, 49 Conn.App. 582, 590–91, 715 A.2d 807 (1998). Finally, “[o]ur review of the trial court’s decision to grant [a] motion for summary judgment is plenary. . . . Moreover, [c]onstruction of a contract of insurance presents a question of law for the court which this court reviews de novo.” (Citation omitted; internal quotation marks omitted.) *R.T. Vanderbilt Co. v. Continental Casualty Co.*, 273 Conn. 448, 456, 870 A.2d 1048 (2005).

## I

[12] We first address the issue of whether the defendants have waived their coverage defenses. The plaintiffs contend that the trial court erred in ruling that the defendants did not have a duty to defend. The trial court found, on the basis of the policy, that the defendants had not breached their duty to defend, and consequently, had not waived their coverage defenses pursuant to our Supreme Court’s ruling in *Black v. Goodwin, Loomis & Britton, Inc.*, 239 Conn. 144, 160, 681 A.2d 293 (1996) (when insurer breaches duty to defend, insurer will be bound when insured enters into settlement agreement in good faith). On the basis of our own construction of the policy, we agree with the trial court.

[13] “Where, as in the present case, an insured alleges that an insurer improperly

6. The parties stipulated that the remaining counts alleged against the defendants are not viable in the absence of a breach of an insurance contract. The trial court rendered judg-

ment in accordance with the parties’ stipulation. Thus, there has been a final judgment for the purposes of this appeal. See Practice Book § 61–3.

has failed to defend and provide coverage for underlying claims that the insured has settled the insured has the burden of proving that the claims were within the policy's coverage....” <sup>1458</sup>*Metropolitan Life Ins. Co. v. Aetna Casualty & Surety Co.*, 249 Conn. 36, 55, 730 A.2d 51 (1999).<sup>7</sup>

The policy provides, in relevant part, that: “[s]ubject to all of the terms and conditions of this insurance, we will have the right and duty to defend the insured against a suit, even if such suit is false, fraudulent, or groundless.” The policy defines a “suit” as “a civil proceeding in which damages, to which this insurance applies are sought ... [and] includes arbitration or other dispute resolution proceeding ... to which the insured must submit or does submit with our consent.”

The plaintiffs’ claim is based on the following additional facts. Following the incident in which the tapes were lost, IBM retained a consultant and took remedial actions. IBM also made a demand against Recall on March 30, 2007, for all of the costs that it incurred or would incur in connection with the lost tapes. Recall, as an additional insured under Ex Log’s policy, notified the defendants of IBM’s demand; however, both of the defendants denied coverage and declined to participate in the negotiations between IBM and Recall. On April 28, 2008, the negotiations concluded and Recall agreed to reimburse IBM \$6,192,468.30.

Recall maintains that it engaged in nearly two years of settlement negotiations—first with IBM, then with Ex Log—and that such negotiations constituted a “suit” or “other dispute resolution proceeding,” which the defendants had a duty to defend. The plaintiffs argue that because the defendants have breached their duty to de-

fend, they are liable for the full amount of Recall’s settlement with IBM. We do not accept this unduly broad reading of the policy.

[14–17] <sup>1459</sup> “[C]onstruction of a contract of insurance presents a question of law for the court which this court reviews de novo.... An insurance policy is to be interpreted by the same general rules that govern the construction of any written contract.... In accordance with those principles, [t]he determinative question is the intent of the parties, that is, what coverage the ... [insured] expected to receive and what the [insurer] was to provide, as disclosed by the provisions of the policy.... If the terms of the policy are clear and unambiguous, then the language, from which the intention of the parties is to be deduced, must be accorded its natural and ordinary meaning.... Under those circumstances, the policy is to be given effect according to its terms.... When interpreting [an insurance policy], we must look at the contract as a whole, consider all relevant portions together and, if possible, give operative effect to every provision in order to reach a reasonable overall result....

[18–21] “In determining whether the terms of an insurance policy are clear and unambiguous, [a] court will not torture words to import ambiguity where the ordinary meaning leaves no room for ambiguity.... Similarly, any ambiguity in a contract must emanate from the language used in the contract rather than from one party’s subjective perception of the terms.... As with contracts generally, a provision in an insurance policy is ambiguous when it is reasonably susceptible to more than one reading.... Under those

7. The settlement agreement between IBM and Recall specifically did not waive Recall’s liability to IBM for “any future claim by IBM for

indemnity from Recall for monetary damages paid by IBM....”

circumstances, any ambiguity in the terms of an insurance policy must be construed in favor of the insured because the insurance company drafted the policy. . . . This rule of construction may not be applied, however, unless the policy terms are indeed ambiguous.” (Internal quotation marks omitted.) *National Grange Mutual Ins. Co. v. Santaniello*, 290 Conn. 81, 88–89, 961 A.2d 387 (2009).

<sup>1460</sup>On the basis of a plain reading of the policy, we cannot conclude that the term “suit” or phrase “other dispute resolution proceeding” was meant to encompass the mere negotiations that took place in this case. First, the plaintiffs fail to cite any authority for this interpretation. Second, such an interpretation would create internal inconsistency within the policy as it would merge the term “claim” with “suit.” For example, under the express terms of the policy, the insured owes a duty to the insurer to provide notice of both “claims” and “suits,” but the insurer only has the duty to defend against “suits.” Our Supreme Court has held that “a demand letter from a potential plaintiff in a personal injury action is a claim. Such a demand letter falls short of a suit, broadly defined as ‘an attempt to recover a right or claim through legal action’ . . . because it has no immediate legal effect and therefore cannot be considered legal action.” (Citation omitted; emphasis omitted.) *R.T. Vanderbilt Co. v. Continental Casualty Co.*, *supra*, 273 Conn. at 469, 870 A.2d 1048.

[22] Thus, to construe “suit” to include mere negotiations following a demand, would obliterate the distinction between “suit” and “claim.” This construction must be rejected. “A construction of an insurance policy which entirely neutralizes one provision should not be adopted if the contract is susceptible of another construction which gives effect to all of its provisions and is consistent with the general intent.”

(Internal quotation marks omitted.) *Hansen v. Ohio Casualty Ins. Co.*, 239 Conn. 537, 548, 687 A.2d 1262 (1996).

We also share the concern articulated in the trial court’s memorandum of decision: “If the [settlement negotiations] [were] found to be an ‘other dispute resolution proceeding,’ every discussion, however informal, between an insured and a third party could be deemed a dispute resolution proceeding.” We decline to give <sup>1461</sup>the word “suit” such an expansive reading so at odds with its usual usage.

[23] Finally, even if the phrase “other dispute resolution proceeding” included the negotiations that took place in the present case, this alone would not trigger the duty to defend as the policy requires that the defendants consent to the proceeding. As there is no genuine issue of material fact that the defendants did not consent to the negotiations, the duty to defend was not triggered. We agree with the trial court that the defendants have not breached their duty to defend and thus have not waived their coverage defenses.

## II

[24] We next address the plaintiffs’ claim that the trial court erred in its interpretation of the policy. The plaintiffs maintain that the personal injury provision in the policy covered the cost of notifying the affected employees following the loss of the tapes. Specifically, the plaintiffs claim that (A) the loss of the tapes constitutes personal injury as defined in the policy, and (B) the loss of the tapes triggered the remedial provisions of certain state privacy laws, such that personal injury can be presumed. We disagree.

## A

In determining whether the trial court properly concluded that there was no cov-

erage under the personal injury provision of the policy, we must examine the language of the policy as it applies to the facts alleged in the pleadings and averred in the parties' affidavits submitted in conjunction with the summary judgment proceedings. See *Missionaries of the Co. of Mary, Inc. v. Aetna Casualty & Surety Co.*, 155 Conn. 104, 110, 230 A.2d 21 (1967). In interpreting the language of the policy, we rely on the principles of construction as set forth in part I of this opinion.

<sup>1462</sup>The policy provides, in relevant part: "[W]e will pay damages that the insured becomes legally obligated to pay by reason of liability: imposed by law; or assumed in an insured contract; for advertising injury or personal injury to which this coverage applies." The policy defines "personal injury" as: "injury, other than bodily injury, property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other *publication* of material that . . . violates a person's right to privacy." (Emphasis added.)

Turning to the complaint, the plaintiffs allege: "[b]y virtue of the loss and theft of the IBM tapes . . . the personal information that was stored on the tapes, including social security information and other private data, has been *published* to the thief and/or other persons unknown . . . thereby subjecting [the plaintiffs] to potential claims and liability . . . including liability for the cost of notifying the persons whose data was lost and for providing credit monitoring services to persons who requested it." (Emphasis added.)

On the basis of our review of the policy, we conclude that personal injury presupposes *publication* of the personal information contained on the tapes. Thus, the

dispositive issue is not loss of the physical tapes themselves; rather, it is whether the information in them has been *published*. The plaintiffs contend that the mere loss of the tapes constitutes a publication, and has alleged that the information was *published* to a thief. The plaintiffs have failed to cite any evidence that the information was published and thereby failed to take their allegation beyond the realm of speculation. See, e.g., *Norse Systems, Inc. v. Tingley Systems, Inc.*, supra, 49 Conn.App. at 591, 715 A.2d 807 (speculation or conjecture will not overcome motion for summary judgment). As the complaint and affidavits are entirely devoid of facts suggesting that the personal information actually was accessed, there has been no publication.

<sup>1463</sup>The plaintiffs argue that the trial court used an improper definition of publication when it construed the definition of personal injury. In its memorandum of decision, the trial court held that publication required communication "to a third party," adopting the definition of publication our Supreme Court has instructed we use in the defamation context. See *Springdale Donuts, Inc. v. Aetna Casualty & Surety Co. of Illinois*, 247 Conn. 801, 810, 724 A.2d 1117 (1999).

[25] The plaintiffs urge that we adopt the definition of publication set forth in Webster's Third New International Dictionary, which defines publication as the "communication (as of news or information) to the public." Even if we accept this definition, however, our analysis would remain unchanged. Regardless of the precise definition of publication, we believe that access is a necessary prerequisite to the communication or disclosure of personal information.<sup>8</sup> In this regard, the plain-

8. We observe that the term publication may carry slightly different meanings depending on the particular privacy right at issue. As

the precise definition of publication is not essential to our disposition of this appeal, we express no opinion as to whether the trial



tiffs have failed to provide a factual basis that the information on the tapes was ever accessed by anyone.

There is nothing in the record suggesting that the information on the tapes was ever accessed by anyone.<sup>9</sup> A letter from IBM to the affected employees, a copy of which accompanied the affidavit of Dawn Zanfardino, a data privacy manager at IBM, stated: “We have no indication that the personal information on the missing tapes, which are not the type that can be read by a personal computer, has been accessed or has been used for any improper purpose.” Moreover, because the parties stipulated that none of the IBM employees have <sup>1464</sup>suffered injury as a result of the tapes being lost, we are unable to infer that there has been a publication. As there is no genuine issue of material fact that there was publication, we agree with the trial court that the settlement Recall reached with IBM was not covered under the policy’s personal injury provision. See *QSP, Inc. v. Aetna Casualty & Surety Co.*, 256 Conn. 343, 356, 773 A.2d 906 (2001) (“[w]here a plaintiff cannot prove a fundamental element of the underlying tort, e.g., defamation, a claim for personal injury coverage will be denied”).

B

[26] Finally, the plaintiffs claim that certain statutes required IBM to notify its affected employees of the data loss and that the triggering of those statutes are “presumptive invasions of privacy.” Essentially, the plaintiffs contend that when such a notification statute is triggered, there has been an invasion of privacy. We disagree with this logic.

court properly adopted the definition as set forth in *Springdale Donuts, Inc.*, and in the context of defamation.

The plaintiffs cite two statutes, one in New York; N.Y. Gen. Bus. Law § 899-aa (2) (McKinney 2005); and one in Connecticut; General Statutes § 36a-701b; both of which require certain actions be taken when personal information is compromised.

In this case, IBM claims to have suffered a loss of more than \$6 million related to the alleged compliance with these notification statutes. While we do not speculate as to whether these expenditures were required by law, we conclude that they do not constitute a personal injury as defined in the policy. These notification statutes simply do not address or otherwise provide for compensation from identity theft or the increased risk thereof, they merely require notification to an affected person so that he may protect himself from potential harm. Accordingly, merely triggering a notification statute is not a substitute for a personal injury. See, e.g., <sup>1465</sup>*QSP, Inc. v. Aetna Casualty & Surety Co.*, supra, 256 Conn. at 376, 773 A.2d 906 (coverage cannot extend to “other torts, not specifically enumerated, which bear [only] some similarity to those listed in the policy” [internal quotation marks omitted]). We therefore conclude that the trial court properly granted the defendants’ motions for summary judgment.

The judgment is affirmed.

In this opinion the other judges concurred.



9. Indeed, there is nothing in the record that suggests the unknown party even recognized that the tapes contained personal information.

644 Fed.Appx. 245

This case was not selected for publication in West's Federal Reporter.

See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also U.S.Ct. of Appeals 4th Cir. Rule 32.1. United States Court of Appeals, Fourth Circuit.

The TRAVELERS INDEMNITY COMPANY OF AMERICA, Plaintiff–Appellant,

v.

PORTAL HEALTHCARE SOLUTIONS, L.L.C., Defendant–Appellee.

American Insurance Association; Complex Insurance Claims Litigation Association, Amici Supporting Appellant.

No. 14–1944.

Argued: March 24, 2016.

Decided: April 11, 2016.

#### Synopsis

**Background:** Insurer commenced action in diversity seeking declaratory judgment that it did not have duty under insurance policies to defend insured in underlying class action. The United States District Court for the Eastern District of Virginia, [Gerald Bruce Lee, J.](#), 35 F.Supp.3d 765, granted insured's motion for summary judgment, and insurer appealed.

**Holdings:** The Court of Appeals held that:

<sup>[1]</sup> diversity jurisdiction was adequately established; and

<sup>[2]</sup> insurer had duty to defend insured against class action complaint.

Affirmed.

\*245 Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria.

[Gerald Bruce Lee](#), District Judge. (1:13–cv–00917–GBL–IDD).

#### Attorneys and Law Firms

**ARGUED:** [G. Eric Brunstad, Jr.](#), Dechert LLP, Hartford, Connecticut, for Appellant. [John Janney Rasmussen](#), Insurance Recovery Law Group, PLC, Richmond, Virginia, for Appellee. **ON BRIEF:** [Kate M. O'Keeffe](#), Dechert LLP, Hartford, Connecticut; \*246 [John Becker Mumford, Jr.](#), [Kathryn Elizabeth Kasper](#), Hancock, Daniel, Johnson & Nagle, P.C., Glen Allen, Virginia, for Appellant. [Laura A. Foggan](#), [Matthew W. Beato](#), Wiley Rein LLP, Washington, D.C., for Amici Curiae.

Before [KING](#), [DIAZ](#), and [HARRIS](#), Circuit Judges.

#### Opinion

Record supplemented and judgment affirmed by unpublished PER CURIAM opinion.

Unpublished opinions are not binding precedent in this circuit.

#### PER CURIAM.

The Travelers Indemnity Company of America appeals from an order entered in the Eastern District of Virginia directing it to defend its insured, Portal Healthcare Solutions, L.L.C., against a civil lawsuit pending in New York state court. As explained below, we are satisfied to supplement the record on appeal and affirm the judgment on the reasoning of the district court. See *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 35 F.Supp.3d 765 (E.D.Va.2014) (the “Opinion”).

#### I.

On April 18, 2013, Dara Halliday and Teresa Green filed a class-action complaint in New York on behalf of themselves and others (the “class-

action complaint”). The class-action complaint alleges that Portal and others engaged in conduct that resulted in the plaintiffs’ private medical records being on the internet for more than four months. During the alleged tortious conduct, Portal was the insured under two insurance policies issued by Travelers, one that spanned the period from January 2012 to January 2013, and another that ran from January 2013 to January 2014 (together, the “Policies”).

On July 30, 2013, Travelers sued Portal in the Eastern District of Virginia, seeking a declaration that it is not obliged to defend Portal against the claims in the class-action complaint. That is so, Travelers maintains, because the class-action complaint fails to allege a covered publication by Portal. Travelers and Portal each moved for summary judgment on the duty-to-defend issue. On July 17, 2014, the district court ruled from the bench that Travelers is duty bound under the Policies to defend Portal against the class-action complaint. It thus granted summary judgment in favor of Portal, as memorialized in its Opinion. This appeal ensued, and we possess jurisdiction pursuant to 28 U.S.C. § 1291.

## II.

Although not raised in the district court, we noted a potential defect in the declaratory judgment proceedings concerning subject matter jurisdiction. In its complaint for declaratory relief, Travelers avers that it is a Connecticut corporation and that Portal is a limited liability company organized and existing under the laws of Nevada, with its principal place of business in Virginia. According to Travelers, the district court possessed subject matter jurisdiction pursuant to 28 U.S.C. § 1332, based on diversity of citizenship.

<sup>[1]</sup> Because Portal is a limited liability company rather than a corporation, however, its citizenship for purposes of diversity jurisdiction turns not on its place of formation or principal place of business, but on the citizenship of Portal’s members. See *Cent. W. Va. Energy Co. v. Mountain State Carbon, L.L.C.*, 636 F.3d 101, 103 (4th Cir.2011); accord *Johnson v. Columbia Props. Anchorage, L.P.*, 437 F.3d 894, 899 (9th Cir.2006) (collecting rulings of \*247 various courts of appeals that limited liability companies possess

citizenship of their members for purposes of diversity jurisdiction). Neither Travelers’s complaint nor the original record on appeal revealed the citizenship of Portal’s members. Accordingly, on March 9, 2016, our Clerk asked the parties to address subject matter jurisdiction at oral argument.

<sup>[2]</sup> On March 21, 2016, three days prior to oral argument, the parties sought to supplement the record on appeal with a Stipulation, pursuant to [Federal Rule of Appellate Procedure 10\(e\)](#), identifying Portal’s three members and stipulating that one was a citizen of Virginia and that the two others were foreign nationals when Travelers filed its complaint. As a result, Travelers and Portal agreed that they are completely diverse for purposes of § 1332 jurisdiction. Consistent with the statutory prescription that “[d]efective allegations of jurisdiction may be amended, upon terms, in the trial or appellate courts,” see 28 U.S.C. § 1653, we hereby grant the [Rule 10\(e\)](#) motion to supplement the record on appeal. We are now also satisfied that Travelers and Portal have adequately established diversity jurisdiction. See *Trans Energy, Inc. v. EQT Prod. Co.*, 743 F.3d 895, 901 (4th Cir.2014).\*

## III.

<sup>[3]</sup> Turning to the substance of Travelers’s appeal, we commend the district court for its sound legal analysis. The court correctly explained that it was required under Virginia law to “follow the ‘Eight Corners’ Rule” by looking to “the four corners of the underlying [class-action] complaint” and “the four corners of the underlying insurance policies” to determine whether Travelers is obliged to defend Portal. See *Travelers*, 35 F.Supp.3d at 769 (relying on *Fuisz v. Selective Ins. Co.*, 61 F.3d 238, 242 (4th Cir.1995)). The court also made clear that, “[u]nder Virginia law, an insurer’s duty to defend an insured ‘is broader than its obligation to pay’ or indemnify an insured,” see *id.* (quoting *Brenner v. Lawyers Title Ins. Corp.*, 240 Va. 185, 397 S.E.2d 100, 102 (1990)), and that the insurer must “use ‘language clear enough to avoid ... ambiguity’ if there are particular types of coverage that it does not want to provide,” see *id.* (quoting *St. Paul Fire & Marine Ins. Co. v. S.L. Nusbaum & Co.*, 227 Va. 407, 316 S.E.2d 734, 736 (1984) (per curiam)).

<sup>[4]</sup> Applying the foregoing principles, the Opinion

concluded that the class-action complaint “at least potentially or arguably” alleges a “publication” of private medical information by Portal that constitutes conduct covered under the Policies. *See Travelers*, 35 F.Supp.3d at 771 (internal quotation marks omitted). Such conduct, if proven, would have given “unreasonable publicity to, and disclose[d] information about, patients’ private lives,” because any member of the public with an internet connection could have viewed the plaintiffs’ private medical records during the time the records were available online. *See* \*248 *id.* at 772 (internal quotation marks omitted and alteration in original).

Put succinctly, we agree with the Opinion that Travelers has a duty to defend Portal against the class-action complaint. Given the eight corners of the pertinent documents, Travelers’s efforts to parse alternative dictionary definitions do not absolve it of the duty to defend Portal. *See Seals v. Erie Ins. Exch.*, 277 Va. 558, 674 S.E.2d 860, 862 (2009) (observing that the courts “have been

consistent in construing the language of [insurance] policies, where there is doubt as to their meaning, in favor of that interpretation which grants coverage, rather than that which withholds it” (quoting *St. Paul Fire & Marine Ins. Co.*, 316 S.E.2d at 736)).

Having carefully assessed the record and the written submissions, together with the argument of counsel, we discern no error. We are therefore content to affirm the judgment on the reasoning of the district court.

*RECORD SUPPLEMENTED AND JUDGMENT AFFIRMED.*

#### All Citations

644 Fed.Appx. 245

#### Footnotes

- \* It is not uncommon that litigants and trial courts fail to identify and litigate jurisdictional issues. *See, e.g., Stahle v. CTS Corp.*, 817 F.3d 96, 100 n. 1 (4th Cir.2016). In such circumstances, certain of our sister circuits remand “for further development of the jurisdictional record.” *See Siloam Springs Hotel, L.L.C. v. Century Sur. Co.*, 781 F.3d 1233, 1239 (10th Cir.2015); *Rolling Greens MHP, L.P. v. Comcast SCH Holdings L.L.C.*, 374 F.3d 1020, 1020–21 (11th Cir.2004) (per curiam). We encourage litigants and their counsel—as well as the district courts—to resolve jurisdictional omissions promptly, before addressing other aspects of disputes that the federal courts may lack the power to decide. *See United States v. Wilson*, 699 F.3d 789, 793 (4th Cir.2012) (explaining that, absent subject matter jurisdiction, “a court can only decide that it does not have jurisdiction”).

# SUPREME COURT OF THE STATE OF NEW YORK NEW YORK COUNTY

PRESENT: JEFFREY K. OING  
J.S.C. Justice

PART 48

Index Number : 651982/2011  
ZURICH AMERICAN INSURANCE  
vs  
SONY CORPORATION OF AMERICA  
Sequence Number : 014  
PARTIAL SUMMARY JUDGEMENT

INDEX NO. \_\_\_\_\_

MOTION DATE \_\_\_\_\_

MOTION SEQ. NO. \_\_\_\_\_

The following papers, numbered 1 to \_\_\_\_\_, were read on this motion to/for \_\_\_\_\_

Notice of Motion/Order to Show Cause — Affidavits — Exhibits \_\_\_\_\_ No(s). \_\_\_\_\_

Answering Affidavits — Exhibits \_\_\_\_\_ No(s). \_\_\_\_\_

Replying Affidavits \_\_\_\_\_ No(s). \_\_\_\_\_

Upon the foregoing papers, it is ordered that this motion is

*Mtn for summary judgment denied  
Xmtns for summary judgment granted.*

*The reasons for the decision & order are  
set forth on the 2/21/14 record and are  
incorporated herein for all purposes.*

*II Zurich directed to order the transcript  
& submit it to the Court to be so ordered.*

Dated: 2/21/14

  
JEFFREY K. OING, J.S.C.  
J.S.C.

1. CHECK ONE: ..... ☐ CASE DISPOSED ☒ NON-FINAL DISPOSITION
2. CHECK AS APPROPRIATE: ..... MOTION IS: ☐ GRANTED ☐ DENIED ☐ GRANTED IN PART ☒ OTHER
3. CHECK IF APPROPRIATE: ..... ☐ SETTLE ORDER ☐ SUBMIT ORDER
- ☐ DO NOT POST ☐ FIDUCIARY APPOINTMENT ☐ REFERENCE

MOTION/CASE IS RESPECTFULLY REFERRED TO JUSTICE  
FOR THE FOLLOWING REASON(S):

1

1  
2 SUPREME COURT OF THE STATE OF NEW YORK  
3 COUNTY OF NEW YORK: CIVIL TERM: PART - 48

4 -----X  
5 ZURICH AMERICAN INSURANCE COMPANY,  
6 Plaintiff

INDEX NUMBER:  
651982/2011

7 -against-

8 SONY CORPORATION OF AMERICA, SONY COMPUTER ENTERTAINMENT AMERICA  
9 LLC, SONY ONLINE ENTERTAINMENT LLC, SONY NETWORK ENTERTAINMENT  
10 INTERNATIONAL LLC, SONY NETWORK ENTERTAINMENT AMERICA, INC.,  
11 MITSUI SUMITOMO INSURANCE COMPANY OF AMERICA, NATIONAL UNION  
12 FIRE INSURANCE COMPANY OF PITTSBURGH, PA., ACE AMERICAN  
13 INSURANCE COMPANY, XL INSURANCE COMPANY LIMITED-IRISH BRANCH,  
14 ST. PAUL FIRE AND MARINE INSURANCE COMPANY, GREAT AMERICAN  
15 INSURANCE COMPANY OF NEW YORK, A-K INSURANCE COMPANIES  
16 (FICTITIOUS DEFENDANTS) and L-Z INSURANCE COMPANIES (FICTITIOUS  
17 DEFENDANTS),

Defendants

-----X  
60 Centre Street  
New York, New York 10007  
February 21, 2014

BEFORE:

HONORABLE: Jeffrey K. Oing, JSC

APPEARANCES:

18 Coughlin Duffy, LLP  
19 Attorneys for Zurich American Insurance Company  
20 350 Mount Kemble Avenue, P.O. Box 1917  
Morristown, New Jersey 07962  
By: Kevin Coughlin, Esq.  
Robert Kelly, Esq.

21 Nicolaides Fink Thorpe Michaelides Sullivan, LLP  
22 Attorneys for Mitsui Sumitomo  
23 Insurance Co. Of America  
24 71 South Wacker, Suite 4400  
Chicago, IL 60606  
By: Robert S. Marshall, Esq.  
Amy Klie, Esq.

25  
26 Delores Hilliard  
Official Court Reporter

- OFFICIAL COURT REPORTER

## Proceedings

## APPEARANCES CONTINUED:

Orrick, Herrington & Sutcliffe, LLP  
Attorneys for The Sony Defendants  
51 West 52nd Street

New York, New York 10019

By: Richard DeNatale, Esq.

Stephen G. Foresta, Esq.

Peri N. Mahaley, Esq.

Drinker Biddle & Reath, LLP  
Attorneys for Ace Property Casualty Ins.

500 Campus Drive

Florham Park, New Jersey 07932

By: William T. Corbett, Jr., Esq.

L'Abbate, Balkan Colavita & Contini, LLP  
Attorneys for Great American Ins. Co of New York  
1001 Franklin Avenue

Garden City, New York 11530

By: Dominic M. Pisani, Esq.

Nelson Levine de Luca & Hamilton  
Attorneys for National Union Fire Ins Co of Pittsburgh, Pa

17 State Street, 29th Floor

New York, New York 10004

By: Marc S. Voses, Esq.

Putney, Twombly, Hall & Hirson, LLP  
Attorneys for St. Paul Fire and Marine Insurance Company  
521 Fifth Avenue

New York, New York 10175

By: Thomas A. Martin, Esq.

Meagher & Geer, PLLP  
Attorneys for St. Paul Fire and Marine Insurance Co.  
33 South Sixth Street, Suite 4400  
Minneapolis, MN, 55402

By: Paula Weseman Theisen, Esq.

## Proceedings

COURT CLERK: Index Number 651982/2011.

In the matter of Z U R I C H A M E R I C A N  
I N S U R A N C E C O M P A N Y versus S O N Y  
C O R P O R A T I O N O F A M E R I C A, et al.

THE COURT: Okay. The Court has before it the  
matters of Zurich American Insurance Company versus Sony  
Corporation of America, et al. Index number 651982 of 2011.

I have before me motion sequence number four, which  
is a motion by -- Fourteen. I am sorry, motion sequence  
number 14, which is a motion by the defendants, Sony  
Corporation of America, SCA and Sony Computer Entertainment  
America, SCEA for partial summary judgment on its first  
cross claim and first counter claim for a declaration that  
the defendant, Mitsui Sumitomo Insurance Company of America  
and Zurich are obligated to the defendant in the underlying  
lawsuits arising out of a data breach suffered by The Play  
Station network, Sony On-Line Entertainment Network, in  
April of 2011.

I also have within motion sequence number 14,  
Zurich and Mitsui's cross motion pursuant to CPLR 3212 for  
declarations that I have no duty to the defendant, SCEA and  
SCA, respectively.

Appearances for the record. For the plaintiff.

MR. COUGHLIN: Good morning, your Honor. Kevin  
Coughlin on behalf of Zurich American.



Proceedings

THE COURT: For the defendants.

MR. FORESTA: Good morning, your Honor. Stephen Foresta from Orrick, Herrington and Sutcliffe on behalf of the Sony defendants. With me is Richard De Natale and Peri Mahaley, also from Orrick, Herrington and Sutcliffe.

THE COURT: And for Mitsui.

MR. MARSHALL: Robert Marshall on behalf of the defendant and cross complaint, Mitsui Sumitomo Insurance Company of America.

I also have with me Amy Klie.

THE COURT: Okay. And you, sir?

MR. KELLY: Robert Kelly for Zurich, as well.

THE COURT: Okay. Thank you.

Since you're in the well you might as well tell me what your appearances are.

MR. VOSES: Marc Voses from the firm of Nelson Levine de Luca & Hamilton on behalf of National Union Fire Insurance Company, Pittsburg P.A., in opposition to the motion.

MR. CORBETT: William Corbett on behalf of Ace America Insurance Company.

MS. THEISEN: Paula Weseman Theisen on behalf of St. Paul Fire Insurance Company in opposition to the motion.

THE COURT: I know I have other motions pending.

Since this one was keyed up first I think the

## Proceedings

1  
2 resolution of this motion may take care of the other motions  
3 that are sort of percolating out there.

4 The way I look at it, after we have done this today  
5 I would suggest that we let the dust settle on how this  
6 plays out. And then for you folks we will give you a  
7 control date. Then, at that point we will figure out what  
8 we should do next in terms of how we go about taking care of  
9 this case.

10 So, having said that , okay, we all know what the  
11 underlying facts are in this case.

12 There was a data breach of large scale proportions  
13 which was eclipsed now by the Target data breach, I think.

14 But, suffice it to say there is the lawsuit that is  
15 in California that is going forward.

16 There was an amended consolidated complaint. It  
17 was dismissed.

18 But, then the plaintiffs, the class action filed  
19 another complaint.

20 The Federal Court dismissed certain of those  
21 claims. But, suffice it to say, it is still alive and  
22 percolating out there in California, right, the underlying  
23 complaint?

24 MR. COUGHLIN: Barely so, but alive.

25 THE COURT: Why don't you do this first. Let's  
26 talk about the exclusion.

## Proceedings

1  
2 Because, the way I look at it why talk about  
3 coverage if at the end of the day if I do find coverage  
4 there is an exclusion that kicks in and gets rid of all of  
5 that. So, I want to do the exclusion first.

6 But, the first thing I want to talk about is  
7 Mitsui's argument with respect to SCA is not named in the  
8 amended class action complaint.

9 Is that your argument?

10 MR. MARSHALL: That's correct, your Honor.

11 THE COURT: Did you take a look at the policy  
12 endorsement of your insurance contract?

13 MR. MARSHALL: Which endorsement, your Honor?

14 THE COURT: The one that I have here which listed  
15 Sony Network Entertainment Incorporated International LLC as  
16 well as Sony Online Entertainment LLC.

17 MR. MARSHALL: Yes, they are still the defendants.  
18 That is subject to a separate motion for summary  
19 judgment we filed which has not been briefed yet.

20 THE COURT: But, they are named. Right.

21 So, your argument in here about how there is an  
22 issue about whether or not there is coverage at all because  
23 they are not a policyholder, did I misread that argument?

24 MR. MARSHALL: No.

25 Our argument is that the underlying litigation does  
26 not trigger the defense.

Proceedings

1  
2 And we are responding to, they brought the motion  
3 only on behalf of SCA, not on behalf of Sony Online or Sony  
4 Network Entertainment.

5 So, our argument is that the underlying litigation  
6 does not trigger the personal advertising injury offense.

7 If that is true, then the other motion becomes a  
8 mere formality because it is the same underlying litigation.

9 MR. De NATALE: Your Honor, we think that the  
10 underlying case does clearly cover the privacy coverage that  
11 triggered that duty to defend.

12 THE COURT: You represent all of the Sony entities,  
13 right?

14 MR. De NATALE: That's correct.

15 THE COURT: So, it doesn't matter if you pick and  
16 choose who you prep. The issue is still, my guy has a  
17 policy. The fact that I went with one of my clients as  
18 opposed to the other affiliate client, it doesn't matter.

19 I mean, the bottom line is we have got coverage or  
20 at least we are arguing that we have coverage. And  
21 everybody that is supposed to be on these policies is there.

22 MR. De NATALE: That's correct.

23 THE COURT: That's the bottom line.

24 MR. De NATALE: If there has been any claim it is a  
25 duty to end the entire case. We would have later  
26 proceedings about how much they have to pay for allocation.

## Proceedings

But, that is not before The Court today.

THE COURT: The sense I get is that the vehicle is probably the wrong vehicle. But, nonetheless, it is still one of the vehicles in my lot that I'm pursuing.

And at the end of the day, Judge, the bottom line is that we are going to argue there is coverage. It doesn't matter who pushes the argument, either the parent corporation or the subsidiary. But, we are all covered at the end of the day.

MR. De NATALE: That is our argument, your Honor.

THE COURT: So, that's for the argument later on with respect to the coverage. I just wanted to get that out of the way in terms of exclusions now.

We have one thing where Zurich is saying there is an internet type business exclusion that applies.

Before we get started, I just want to get for the record, Zurich's insurance policy and the Mitsui are identical? I looked through both of them.

MR. COUGHLIN: No. There are differences to that. They were issued separately to different entities.

THE COURT: That's okay. I'm talking about the policy language that is at issue.

MR. COUGHLIN: There is a lot of overlap on the standard wording, the insurance grants, that sort of thing. You're correct in that way.

## Proceedings

1  
2 THE COURT: The particularities that you're  
3 disputing or at least arguing about today are identical?

4 MR. COUGHLIN: Correct.

5 THE COURT: That is important.

6 So, tell me why in terms of the internet type  
7 business? And that would be falling under the B coverage.  
8 B1, J,1,2 and 3.

9 MR. COUGHLIN: Your Honor, would you mind if I took  
10 the podium?

11 THE COURT: Whatever is convenient for you.

12 MR. COUGHLIN: It is necessary for my eyesight.

13 THE COURT: Mine, too.

14 MR. COUGHLIN: Your Honor, let me start, if I may,  
15 with the issue of the exclusion which obviously follows, as  
16 it must, the issues with respect to the insurer's view that  
17 there is a total absence of publication here and coverage B  
18 doesn't apply.

19 THE COURT: Putting that aside for the minute.

20 MR. COUGHLIN: Yes. The issue with the exclusion  
21 is wrapped up, your Honor, with other issues that have  
22 brought us here today that cannot be ignored.

23 And that is, the Zurich policy as well as the  
24 Mitsui policy was never intended to cover cyber losses.

25 THE COURT: You know, whatever your intent is, the  
26 bottom line is that I'm restricted to what the policy terms

## Proceedings

are.

So, you can say intent. We only get to intent if I find there is an ambiguity.

If there is no ambiguity I don't have to go to the intent aspect of what you insurance companies thought you were providing and what the policyholders thought they were getting.

So, the bottom line is I just have to look at what we have here.

MR. COUGHLIN: I agree, your Honor.

THE COURT: So, hearing for the record what the exclusion says, personal and advertising injury, this is excluded. Personal and advertising injuries committed by an insured whose business is.

One and two are out. It is three, which says an internet search access content or service provider.

Now, the question then becomes is Sony or any of the Sony defendants here falling into that category.

MR. COUGHLIN: The answer for today, your Honor --

THE COURT: For today?

MR. COUGHLIN: Is that SCEA is an entity that fits within 3. Because, Sony decided to only move against my client on that entity.

That was a decision they made. So, it is not in front of your Honor today.

## Proceedings

And what is interesting --

THE COURT: You know what, that is interesting that you say that, but for today.

I don't know how you folks want to do it, but I just want to be done with this. There is no today, tomorrow or yesterday.

I mean, I've got the Sony defendants all here. I have all of the insurance carriers here.

So, it is not going to change anything from today or tomorrow if I don't talk about whether or not the defendants, the Sony defendants, fall within the category of paragraph 3 altogether.

MR. De NATALE: Your Honor --

MR. COUGHLIN: The problem --

THE COURT: Hang on.

MR. COUGHLIN: The problem that Sony has put on your Honor's desk this morning --

THE COURT: Well, I think you're all guilty of that.

MR. COUGHLIN: Well, your Honor, respectfully, no.

They chose to move on only two entities. The SCA, parent against Mitsui and SCA against Zurich.

We were, frankly, somewhat mystified that they did it, too. But, they did it.

THE COURT: This is a summary judgment motion, so



## Proceedings

that I can search the record.

So that as long as they are named, as long as they are a named defendant in this case when you move under 3212 I can do a lot of things. I'm not restricted to just the pleadings like a 3211 motion. I can search the record.

And I cannot stick my head in the sand and ignore something when it is jumping out at me.

MR. COUGHLIN: Your Honor, I'm happy to address our view of that.

Sony has taken positions that seem to focus exclusively on SCEA and to the omission of the other entities factually.

But, I'm happy to deal with section 3. Because, your Honor, we don't think there is any question that Sony, and I will use Sony Corp., SCA, SCEA, fits squarely into section 3 of that exclusion.

And what is interesting, your Honor, it wasn't until the summary judgment briefs that we see that the SCEA entities are now alleging it is not to them, technically. And we are really not an entertainment company, we are something else.

But, what is striking here is the public pronouncements by SCEA and Sony after the cyber breach where they were inundated with their concern about the ultimate risk here which thankfully has been de-risked substantially.

## Proceedings

1  
2 But, in those first months they issued press  
3 release after press release about who they are, what they  
4 do.

5 They were terribly concerned because members of  
6 Congress were crying out for an investigation. And the  
7 chairman of SCEA put a submission to them in the form of a  
8 letter describing who they are.

9 THE COURT: So, what you are saying then is because  
10 the defendant, SCEA, is moving for summary judgment and not  
11 the other Sony defendants, we are talking about SCEA, SCA.  
12 So that you are saying that there may be opportunities of,  
13 if I would rule, if you were not to prevail in that argument  
14 here that it is included under paragraph 3, you are saying  
15 that later on you may have an opportunity again because of  
16 the way this is teed up to argue that the other Sony  
17 defendants if they move that they may fall under paragraph  
18 3.

19 MR. COUGHLIN: Well, your Honor, it is this way.

20 It is because the Sony entities have taken a view  
21 in the briefing that SCEA didn't have specific  
22 responsibility for the servers, for the Play Station network  
23 business, etc.. It is in their briefs that way. So, they  
24 tried to carve that out.

25 The other problem confronting us this morning is we  
26 believe all of their public statements, their pronouncements

## Proceedings

1  
2 where they are trying to get a handle on this problem from a  
3 public relations point of view, an over all legal view was  
4 it is SCEA. We are an internet content provider. We  
5 provide all sorts of access, Hulu, Netflix, all of these  
6 other things through the Play Station network to our  
7 subscribers.

8 And it is absolutely clear in those pronouncements.

9 THE COURT: Let me ask you in response to that  
10 question then, that that is sort of like a 3rd party service  
11 that they are doing. So, you're arguing that they fall  
12 under this paragraph 3 exclusionary language.

13 But, that's not the only thing they do.

14 They also do, according to The Federal Court's  
15 decision, which is at 2014 Westlaw 223677, that they also do  
16 in addition to what you just said, which is a 3rd party  
17 services provider.

18 MR. COUGHLIN: By the way, respectfully, I did not  
19 agree with that. I did not say it was a 3rd party service,  
20 your Honor.

21 THE COURT: I'm just using that. I'm using that  
22 analogy from what The Federal Court said here. This is how  
23 The Federal Court describes what Sony does.

24 Sony develops and markets the Play Station portable  
25 hand-held devices, PSP and the Play Station 3 console PSP,  
26 collectively, consoles and all consoles.

## Proceedings

Both consoles allow users to play games, connect to the internet and access, Qriocity -- Q-R-I-O-C-I-T-Y.V

MR. COUGHLIN: Qriocity.

THE COURT: Qriocity. Sony Online Entertainment Services and the Play Station network PVS and collectively through the PSN, which is offered to consumers free of charge. Users can engage in multiple on-line games. And for additional one time fees the PS allows users to purchase video games, add on content defined as Mapsters, demos movies and movies selectively down-loaded. Users can also access various prepaid 3rd party services by connecting to Sony Online Services via their consoles or computers including Netflix, MLV, Dot TV and NSHL game center, collectively, 3rd party services.

Then, this goes on to say, before establishing a PSN Qriocity and/or SOE account plaintiffs and other consumers are required to enter into terms of identifying users with Sony and agree to Sony's privacy policy as part of this registration process.

Plaintiffs and their consumers were required to advise Sony with personal identification information including their names, mailing addresses, e-mail address, birth dates, credit and debit card information, card numbers, expiration dates and security code and log-in credentials, collectively, with personal information.

## Proceedings

Now, I'm looking at that description of what Sony does. This is now in a decision. So, factually, I'm just looking at that for some guidance.

It sounds like they do more than being an internet search, or access, or content or service provider. They are sort of a hybrid. They do a lot of things.

MR. COUGHLIN: They certainly do, your Honor.

THE COURT: This policy doesn't say --

It's very clear as to what it says. It doesn't go on and say, and any other hybrid type of situation.

It's very clear. It lists 3 or 4 instances of internet search, which clearly this description doesn't fall into an internet search. Internet access, okay, internet access.

But, for internet access they do a lot of things, not just pure access.

For example as to Google or some other Internet Explorer, it is not content based in the sense that it is not just there for static information. And it is not a service provider in the sense that, oh, yes, it does service provide, but it allows people who pay up to play games on their Play Stations. So that it is sort of a hybrid.

It doesn't fall into any of these categories here at all.

MR. COUGHLIN: Well, respectfully, Judge, I think

## Proceedings

1  
2 it is a content provider. It is a service provider.

3 THE COURT: In what way?

4 MR. COUGHLIN: And the case law says it doesn't  
5 have to be the only business. It has to be a principal  
6 business.

7 THE COURT: That's not what this says. That is not  
8 what your policy said.

9 MR. COUGHLIN: Your Honor --

10 THE COURT: Where is it in this, your policy, in  
11 that paragraph that you say it is principally what you do?

12 MR. COUGHLIN: It is not there, Judge.

13 THE COURT: Okay.

14 MR. COUGHLIN: But --

15 THE COURT: And we know what the exclusionary  
16 language is.

17 The Court looked at that very carefully. Because,  
18 exclusionary language in a policy is strictly construed.

19 And if there is an ambiguity with respect to an  
20 exclusionary language the ambiguity is resolved in favor of  
21 the policyholder. That is pretty clear.

22 So that when you talk about that I would like you  
23 to point out in paragraph 3 where you get that principal  
24 language.

25 I looked at that policy. I didn't see it.

26 There was a lot of reading last night. Magnifying

## Proceedings

1  
2 glass work.

3 MR. COUGHLIN: Judge, the problem, Judge, and let  
4 me stay just inside of the policy and let me stay with what  
5 Sony has said outside of their briefs.

6 Our exhibit 16 to our motion, my affidavit, Sony  
7 describes the SCEA entity.

8 And they describe it, and it's on page two, that  
9 they operate the Play Station network, which is the access  
10 point.

11 THE COURT: Right.

12 MR. COUGHLIN: And it is a computer entertainment  
13 system and its on-line and network services, The Play  
14 Station network.

15 What I'm coming back to there in this problem, your  
16 Honor, for the reason that their on-line product and  
17 service, which is a significant component to their business,  
18 which if you look at the words of our policy -- and I don't,  
19 respectfully, believe it is just three. I think it is also  
20 paragraph two, sub-paragraph two.

21 THE COURT: Sub-paragraph two provides, designing  
22 or determining content of web sites for others.

23 MR. COUGHLIN: Yes. For their subscribers.  
24 Therein designing the Hulu and the Netflix, those are  
25 components.

26 They have come up with games. They have all

## Proceedings

1  
2 on-line products. A whole menu.

3 And your Honor, that is --

4 THE COURT: But, again, you don't have the word  
5 principally, principally designing or determining. It is  
6 doing a lot of things on this platform that they have.

7 MR. COUGHLIN: That's correct. This on-line  
8 platform, Judge.

9 So, that on-line platform, which is without doubt  
10 from their own witnesses a significant part of their  
11 business. Not the exclusive. We have never said that.

12 But, to say that unless it is the only part of  
13 their business the exclusion should not apply, I think  
14 misreads the intent of the words.

15 THE COURT: No. That's not misreading the intent  
16 of the words. That is just reading it on face value what  
17 the words say.

18 Because, there are issues in terms of these  
19 policies here.

20 And what you're asking me to do is you're asking me  
21 to read this, these straight forward words, unambiguous  
22 words. You're asking me to read this your way of saying  
23 that, well, it doesn't mean that's exclusively what they  
24 have to do, but principally what they have to do.

25 There is no such wording in here that says, either  
26 principally or exclusively.



## Proceedings

But, you're asking me to read this that way.

MR. COUGHLIN: Correct.

THE COURT: And I cannot read this that way.  
That's not what it says.

MR. COUGHLIN: Your Honor, what Zurich is asking is  
that that exclusion be applied to the stated business of  
SCEA. That is our position, your Honor.

THE COURT: Okay.

MR. COUGHLIN: Not their's, our's.

THE COURT: Your response?

MR. De NATALE: Your Honor, this is an exclusion we  
are talking about. So, it has to be written out.

Zurich has a burden of proof to put in facts.

What they have done, they have pulled some  
statement out of a letter taken out of context and using it  
as some kind of admission.

We put facts in the record about what SCEA Sony  
Computer does. They make the Play Station.

The first Play Station that came out wasn't even  
connected to the internet.

THE COURT: I know.

MR. De NATALE: Most people still use it as a  
stand-alone product.

It does have wi fi access. But, we showed in our  
papers, in fact, 90 percent of the company's revenues have

## Proceedings

nothing to do with the internet or its profits have nothing to do with the internet.

The exclusion has to be applied on a company by company basis.

THE COURT: Yes.

What about their argument? He is saying that you're moving under this summary judgment, but SCA and SCEA and not the other Sony defendants.

So, for today only we are only going to be talking about this exclusionary language.

MR. De NATALE: I will be candid about that.

We brought this motion on behalf of two companies that we thought under no possible conception should be within the internet business exclusion.

We thought we would get a quick hearing. We were hoping to avoid any discovery.

The insurers insisted on taking all of this discovery and went through all of our files to try to prove the internet business exclusion.

They weren't able to come up with anything.

MR. MARSHALL: Your Honor --

THE COURT: Easy there, counsel. Relax.

MR. De NATALE: But, our motion seeks to establish coverage for all of the entities.

MR. MARSHALL: That's not --

## Proceedings

1  
2 MR. De NATALE: Counsel, give me the courtesy,  
3 please.

4 THE COURT: You've had too much coffee. Relax.

5 I give everybody an equal opportunity to be heard.

6 MR. De NATALE: Our motion seeks to establish the  
7 underlying cases allege a publication of private material.

8 THE COURT: I don't want to get into that now.

9 MR. De NATALE: That would apply to everyone.

10 But, on the exclusion we only moved on behalf of  
11 the two companies who under no conceivable way fall within  
12 the exclusion.

13 Later in the case they can try to show that the  
14 other two Sony defendants fall within the exclusion.

15 I think they will fail. But, that would be an open  
16 issue later in the case.

17 MR. MARSHALL: I think he clarified it.

18 Procedurally, Sony filed its motion for partial  
19 summary judgment on behalf of two entities, only. They  
20 weren't seeking coverage from all Sony entities.

21 They did so because they thought they had the best  
22 chance to avoid the exclusion on those two entities.

23 THE COURT: Okay.

24 MR. MARSHALL: After they filed that motion The  
25 Court allowed us to conduct discovery with respect to  
26 application of the exclusion.

## Proceedings

1  
2 So, that's why this is being briefed in two stages.  
3 Meaning, SCA, SCEA first. And then later we filed a motion  
4 for a summary judgment with respect to the on-line company  
5 and the network company. Because, there was discovery  
6 ongoing. And that's why it's separate.

7 So, that hearing should not decide coverage with  
8 respect to the on-line entity.

9 THE COURT: So far the issue that I have in front  
10 of me with respect to the exclusion is limited to SCA and  
11 SCEA.

12 And any ruling I make at this point on going  
13 forward even with respect to coverage, even with respect  
14 to-- I mean, when we get into the arguments with the  
15 coverage issue it's only as to, as Mr. Coughlin indicated  
16 being pressed, is only involving SCA and SCEA; correct?

17 MR. MARSHALL: Okay. I'm fine with that, your  
18 Honor.

19 THE COURT: This is evolving into a situation  
20 where, okay, if I have it for another day it will be teed up  
21 for another argument. It will be teed up for another  
22 argument.

23 MR. De NATALE: One last application.

24 SCA, Sony Corporation of America, there is no  
25 argument with respect to the exclusion. For SCA, Sony  
26 Corporation of America, the exclusion is irrelevant.

## Proceedings

1  
2 THE COURT: SCA. But, SCEA is in the mix. That's  
3 where Zurich is making the argument.

4 MR. MARSHALL: SCA had nothing to do with the  
5 network issues, so we don't make any arguments.

6 THE COURT: You know, I've heard the arguments  
7 here. I'm not convinced at this point that paragraph three  
8 that is involved here or paragraph two that is involved here  
9 with respect to -- I mean, paragraph two.

10 Let me just say this right here. It says, right  
11 here, I am sorry to repeat it for the record.

12 J, the heading for J is insurance in media and  
13 internet type businesses. Personal and advertising injury  
14 committed by an insured whose business is, and paragraph  
15 two, is being put in play, designing or determining content  
16 of web sites for others. Or three, and internet search  
17 access content or service provider.

18 I've heard the arguments here. And when you read  
19 this there is no qualifying language in this exclusionary  
20 clause here. It doesn't say principally. It doesn't say  
21 exclusively. It just lays out the words here in front of  
22 me. And it's very clear.

23 Under the facts that I have for SCEA, the defendant  
24 SCEA, it is clear. It is not just this.

25 Paragraph two and paragraph three does not come  
26 into mind at this point.

## Proceedings

1  
2 Because, I'm looking at The Federal Court's  
3 decision in terms of the description. Because, The Federal  
4 Court in The Judge's decision, Judge Battaglia's decision, a  
5 very thoughtful decision, he defines or at least he sort of  
6 describes what SCEA does. Because, he names SCEA right in  
7 the beginning of describing who the defendants are in this  
8 case.

9 And it gives me the sense that this is a hybrid  
10 situation where it does a lot of things, SCEA. It is not  
11 just limited to what is going on here in this exclusionary  
12 language.

13 So that when you don't have the qualifying language  
14 of exclusively or principally, although Mr. Coughlin,  
15 counsel is arguing that that's what is at play here, I'm not  
16 going to read in a term here that doesn't belong.

17 So, under those circumstances I don't find that SCA  
18 is not involved or implicated in this issue here.

19 But, I don't find SCEA falls within the  
20 exclusionary language that is set forth in this policy that  
21 I have in front of me.

22 As I said earlier, the case law is very clear.  
23 When you come to the exclusionary language it is read very  
24 strictly. It is construed strictly. There is no, I do not  
25 find any ambiguity here.

26 Under those circumstances, I don't find the

## Proceedings

1  
2 exclusion of J2 or J3 applicable to the defendant SCEA.

3 So, that's my decision with respect to that first  
4 issue.

5 Let's turn to the second issue, recording and  
6 distribution of material or information in violation of the  
7 law of exclusion.

8 That is your argument. That is Mitsui's argument,  
9 isn't it?

10 MR. MARSHALL: No.

11 THE COURT: I thought you wrote that in your demand  
12 for denial for coverage? No?

13 MR. MARSHALL: That's not the basis for our summary  
14 judgment motion.

15 THE COURT: That was in your denial letter. But,  
16 that's not being pressed here?

17 MR. MARSHALL: That is not part of our motion for  
18 summary judgment.

19 THE COURT: Then, the next one is the criminal  
20 acts. Same thing?

21 MR. MARSHALL: Not part of the issue.

22 THE COURT: That's not part of it, either? I just  
23 wanted to get that out there.

24 MR. MARSHALL: I can probably kind of cut to the  
25 chase, your Honor.

26 The only basis upon which Mitsui moves for partial

## Proceedings

summary judgment is the fact that the publication of the personal advertising injury offense is not satisfied by the allegations of the underlying litigation.

THE COURT: All right. We are going to get to that in a minute. That's how we are going to get to the heart of it.

I have taken care of all of the exclusion stuff. Now, we are going to get to the coverage stuff here.

And I will turn to the Sony defendants to start that argument as to why they think there is coverage under this policy for what we have here.

MR. De NATALE: Thank you, your Honor.

For more than 20 years insurance companies in The United States have sold general liability policies just like the ones your Honor has before it that include coverage for privacy claims.

The clauses there are written broadly. It's intended to cover many types, a wide variety of privacy torts.

The clause has no limitations or restrictions that depend upon who makes the disclosure, how the material is disclosed or to how many people the material is disclosed.

And under New York law, since it is part of an insurance clause it must be issued broadly.

That's what the courts have done. The courts have



## Proceedings

1  
2 applied that clause to that wide variety of situations where  
3 there is a disclosure of private information or unauthorized  
4 access to private information.

5 In the year 2000 the language of this clause was  
6 expanded to make clear that it covered the internet. And  
7 that's the nature of insurance.

8 The world changes. New torts are being alleged all  
9 of the time. And old policies have to be adopted to cover  
10 new situations.

11 THE COURT: All right.

12 The provision here that is in dispute is in the  
13 definition section.

14 MR. De NATALE: Yes.

15 THE COURT: That's in the definition section 5.

16 We go to paragraph 14. And I will state for the  
17 record what paragraph 14 says.

18 Paragraph 14. (Reading). Personal and advertising  
19 injury means injury including consequential bodily injury  
20 arising out of one or more of the following offenses which  
21 provides, which there is coverage for.

22 A, false arrest, detention or imprisonment.

23 B, malicious prosecution.

24 C, the wrongful eviction from wrongful injury into  
25 or invasion of the right of private occupancy of a room,  
26 dwelling or premises that a person occupies committed by or

## Proceedings

on behalf of its owner, landlord or lessor.

D, oral or written publication in any manner of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services.

E, oral or written publication in any manner of the material that violates a person's right of privacy.

And F, the use of another's advertising idea in your advertisement.

G, infringing upon another's copyright, trade, dress or slogan in your advertisement.

And that is it. Right? That is it.

So, the focus now is, the dispute that we have here is the definition or is focused on E, which is oral or written publication in any manner of material that violates a person's right or privacy.

The case law out there is clearly, or at least not clearly, but having to do with pollution cases.

I haven't seen any data breach case of this magnitude involving this kind of policy.

And the courts haven't addressed this yet. It seems like this is the first one that has come up.

MR. De NATALE: Your Honor, there have been cases addressing all kinds of similar issues, unauthorized access.

THE COURT: Not like this nature where you had a

## Proceedings

hacking into the system.

MR. De NATALE: I agree.

THE COURT: But, a lot of the other cases that we have seen have talked about environmental impact, pollution cases.

They all basically say it is not the 3rd party act that gets you coverage, but it has to be the policyholder/insurer's acts for you to get coverage, for coverage to apply.

MR. De NATALE: So, your Honor, the pollution cases that you're talking about are under section C, the wrongful injury prong. And nothing to do with the privacy prong.

If you see under section C, your Honor, there are additional words in that provision that say committed by or on behalf of owner, landlord or lessor. That is usually the policyholder.

In section C they added words saying the offense has to be committed by the policyholder.

THE COURT: But, aren't there cases out there that said - I looked at some, I don't remember what they are - but they kind of grouped A through E together and said this all has to be done by a policyholder. It cannot be affording coverage when this happens when a third party intervenes or does something.

MR. De NATALE: Your Honor, only under The County

## Proceedings

of Columbia case. The cases don't say that under the privacy prong.

I think each one has to be considered separately.

This is a duty to the defendant motion.

And your Honor is well aware that the duty to defendant is exclusively broad in New York. Coverages are read broadly and the complaints are read broadly, here's what we have been sued for. In the underlying cases there are many, many examples.

The chief complaint says that Sony disclosed private information to unauthorized parties and invaded plaintiff's privacy.

The Deiter (phonetics) case says the same thing.

The complaint says that millions of customers had their financial data compromised and had their privacy rights violated.

There are five other complaints that say the same thing.

The John's (phonetics) complaint says this action is brought to address the defendant, Sony's, violations of consumers right of privacy. There are five other cases that say the same thing.

The NBL (phonetics) case, when it was all consolidated in a multi-district proceeding says that Sony breached the duty of care to protect personal information

## Proceedings

1  
2 from being disclosed to unauthorized parties and placed  
3 sensitive information in the hands of cyber hackers.

4 The amended NBL complaint, the most recent one, in  
5 four different places says the class members have suffered a  
6 loss of privacy.

7 These are the allegations, your Honor.

8 THE COURT: But, you're looking at those  
9 allegations in a vacuum. Because, the totality is that the  
10 hackers, that your security features weren't sufficient to  
11 prevent hackers from coming in and getting access.

12 While the plaintiffs have to say that you guys  
13 breached the duty to them, I mean, they are not going to sue  
14 the hackers because they cannot find the hackers. They can  
15 find the guy that had all of the information. That's you.

16 So, they are coming in and they hacked into your  
17 security system.

18 So, Sony is the victim here.

19 MR. De NATALE: We are the victim, but being sued.

20 THE COURT: You're being sued by others.

21 But, the question is, does this policy prevent,  
22 does this policy provide you coverage for you being the  
23 victim rather than being the perpetrator.

24 MR. De NATALE: Right.

25 So, we are being sued on this allegation that we  
26 collected people's private information, implemented security

## Proceedings

1  
2 factors that they claimed was inadequate that resulted in  
3 that disclosure of millions of people.

4 THE COURT: But, you didn't disclose. It wasn't  
5 your act of disclosure. Someone broke into your --

6 Who used the analogy of a bank robber going into a  
7 bank and taking money as being an unauthorized ATM  
8 withdrawal?

9 I mean, that is not your fault.

10 MR. De NATALE: And the policy grants coverage for  
11 publication in any manner of material that violates the  
12 right of privacy.

13 It doesn't say it has to be publication by the  
14 policyholder. It says in any manner.

15 And I think that is inconsistent with -- If they  
16 wanted to write a clause that says publication committed by  
17 the policyholder they could have done that. That's what  
18 they did in section C.

19 But, what they wrote in a clause that says  
20 publication in any manner, I think that's inconsistent with  
21 reading an implied requirement here that it has to be by the  
22 policyholder.

23 New York law doesn't allow implied exclusions.

24 THE COURT: F and G is also new, too. Because, I  
25 think, virtually all of the cases that I looked at dealt  
26 with A through E. No one talked about F and G.

## Proceedings

1  
2 I think F and G is a new insert in the CGL that  
3 hasn't been discussed yet.

4 MR. De NATALE: There used to be a separate, a  
5 separation of advertising injury and personal injury. They  
6 were combined together and F and G got added.

7 THE COURT: But, the interplay, I was curious to  
8 see what the interplay was or how courts review having F and  
9 G. How that would impact any of the A through E type of  
10 discussions that we have.

11 MR. De NATALE: Your Honor, may I point you to  
12 another provision?

13 I have a hand-out here, if that would be helpful to  
14 The Court, that blows up the language.

15 MR. COUGHLIN: I want to see the exhibit.

16 MR. De NATALE: It is section 1B of the policy.

17 THE COURT: 1B in the front?

18 MR. De NATALE: Yes, in the personal and  
19 advertising.

20 (Handed)

21 THE COURT: Hang on a second.

22 (Peruses)

23 THE COURT: Yes, I've got it.

24 MR. De NATALE: The reason this is important, your  
25 Honor, is that I want to be clear.

26 There are expressed requirements contained in this

## Proceedings

coverage part A. They are here in paragraph 1B.

It says the insurance applies to personal and advertising injuries caused by an event or arising out of a business.

That is one requirement. It has to arise out of a business.

But, only if the offense was committed in the coverage territory. In the coverage territory, which is defined to be for internet offenses any part of the world.

And third, it has to be during the policy period. That's the third requirement.

It doesn't say by the policyholder. It doesn't say it has to be intentional and not negligent.

If the insurers wanted to write express requirements this is the place to put them.

They put three in here. We have met all three.

And now they are trying to re-imply restrictions in requirements which are just not in the text.

New York law doesn't let you do that.

THE COURT: But, you know, the problem with that argument is that when you say this insurance applies to, quote, "personal and advertising injury," unquote, what is that defined as?

You go here and look at paragraph 14 and that defines it. So, everything in paragraph 14 gets thrown in.



## Proceedings

1  
2 MR. De NATALE: Absolutely.

3 But, no where in 1B or 14 does it say it has to be  
4 by the policyholder. It just doesn't say that.

5 And you know, we use an example --

6 THE COURT: This doesn't say that. But this is a  
7 CGL policy that you've already said it's an insurance policy  
8 that insures the policyholder against its acts or acts of  
9 its employees or affiliates. You know, this covers all of  
10 those for their acts.

11 So that you're telling me now that that's not what  
12 it is? It actually embraces actions from 3rd parties in a  
13 hacker situation?

14 MR. De NATALE: The coverage for your acts, your  
15 Honor. But, it covers you for acts of negligence.

16 CGL policies traditionally covers you for acts of  
17 negligence.

18 If someone falls on your premises you haven't  
19 pushed them over.

20 THE COURT: By that argument, doesn't that expand  
21 the liability of the insurance company?

22 That's not what they bargained for. They are  
23 bargaining with the policyholder.

24 MR. De NATALE: Your Honor, absolutely, it's what  
25 they bargained for. It turns insurance on its head.

26 Insurance typically covers your negligence. When

## Proceedings

1  
2 someone slips and falls because your sidewalk is wet or when  
3 you build improperly and something falls down, that is  
4 negligence. And you're covered for your negligence.

5 THE COURT: That's why if you have those kinds of  
6 situations -- Let's go to construction contracts, for  
7 example.

8 You know, a contractor takes out an insurance. The  
9 insurance policy is not going to cover the sub. The sub has  
10 to name the contractor in their policy.

11 MR. De NATALE: But, the contractor can sue for the  
12 sub's negligence. The contractor is covered, it is. That's  
13 section 8 of property damage.

14 But, under section B, absent some express language  
15 that bars coverage for negligence, and there isn't any, it  
16 should be covered, your Honor.

17 And all of the other restrictions that they just  
18 want to, they turn the insurance on its head by reading this  
19 narrowly.

20 Let's talk about the word publication, which has  
21 been a big focus in that case.

22 The insurers say publication means only one thing,  
23 wide spread disclosure to the general public in the sense of  
24 a public announcement or a publication of a book or  
25 magazine. Those are meanings of the word.

26 But, there are other meanings of the word that are

## Proceedings

1  
2 narrower and simple and have the straight forward meaning of  
3 a disclosure, a statement or a disclosure.

4 If you look at Nisarrels (phonetics), we cite in  
5 our brief synonyms for publication are to disclose or simple  
6 disclosure. Black Law dictionary.

7 THE COURT: The term publication is very broad. I  
8 think the term disclosure is more narrow.

9 Disclosure is something where I think the person  
10 that has the information does something to disclose. I  
11 means, that's something.

12 Publication, I think, contemplates a situation  
13 where anybody and everybody can sort of get something out  
14 there, like the defamatory statements.

15 You have a publication. It is not necessarily the  
16 person that is actually doing the defaming that publicizes.  
17 Somebody else can pick it up and publicize it. Then, that  
18 person who actually wrote the piece can be sued for  
19 defamation. But, they didn't publish it. Somebody else  
20 published it and they got it out there. That's how you link  
21 up in terms of publication.

22 In my mind it's more broad. It doesn't necessarily  
23 mean that it is restricted to the actual wrong doer or tort  
24 feator.

25 But, disclosure is a little bit different, a little  
26 more narrow.

## Proceedings

1  
2 MR. De NATALE: I think you can have a negative  
3 publication and you certainly can in a defamation context.  
4 That's the immediately previous paragraph that your Honor  
5 saw the same phrase, publication in any manner is used in a  
6 defamation clause and also used in the proxy clause. This  
7 must mean more or less the same thing.

8 And the restatement of defamation, your Honor,  
9 under the very interesting example of a cartoonist who wrote  
10 a defamatory cartoon and leaves it on his desk where  
11 co-workers go by and see it. And they see this person is  
12 defamed. That's a negligent publication of defamatory  
13 material, because the person allowed access to that  
14 defamatory material to others. And the victim was then  
15 defamed.

16 THE COURT: You know, the Butts case, the West  
17 Virginia case, it is not so bad what this says.

18 I mean, I know, you didn't --

19 MR. De NATALE: We don't like this.

20 THE COURT: You know, you should not be so quick to  
21 not like this. Because, what this did here is very  
22 interesting.

23 They talked about D and E in their decision.

24 The standard for D, the publication was not done by  
25 the defendant company. The publication was done by the  
26 doctor and an employee. More specifically, the doctor who

## Proceedings

1  
2 examined the injured plaintiff. And he put a report out  
3 there that the plaintiff said was defamatory.

4 So, with respect to D, and clearly that is not a  
5 situation where the insured, the policyholder made the  
6 publication, but it was the doctor. They said that was  
7 fine. They said that there is coverage or the duty to  
8 defend in that situation.

9 Before, for E they said that for E they needed  
10 somebody. They needed the actual person to do it. The  
11 policyholder had to do it for E.

12 So, I looked at that and I said, okay, they split  
13 this, D and E. They split it, saying that on the one hand  
14 they're saying you don't have to have the policyholder for  
15 D. But, on E they are saying you do have to have the  
16 policyholder act, to do the act.

17 I examined D and E very carefully. I looked at the  
18 D and E here. There is a big difference there.

19 D and E in my case here has "in any manner." It's  
20 very expansive.

21 MR. De NATALE: That's not in the Butts case;  
22 that's correct. That is not in the Butts case.

23 THE COURT: Not such a bad case.

24 MR. De NATALE: And it is not in The County of  
25 Columbia case either.

26 That's the case they rely on for that notion that

## Proceedings

1  
2 all of the courts require purposeful conduct and insurance  
3 only covers purposeful conduct.

4 The County of Columbia case, that case is focused  
5 on pollution. And this does make a statement about all of  
6 these clauses. But, it is really about the wrongful injury  
7 clause.

8 And that case was decided before this coverage was  
9 even part of the standard policy with endorsement and before  
10 the words "in any manner" came in.

11 THE COURT: I have got it. Have a seat.

12 Your response, Mr. Coughlin?

13 The "in any manner" is pretty broad don't you  
14 think? This is not the typical kind of language that I have  
15 seen in all of the other cases.

16 MR. MARSHALL: I just have to clarify one thing.  
17 We are getting ahead of ourselves.

18 THE COURT: I'm not getting ahead of myself.

19 MR. MARSHALL: When we are talking about the  
20 insured published anything, we are assuming that the  
21 underlying complaints are alleging that the hackers  
22 published something. But, it doesn't allege that.

23 THE COURT: I didn't assume that.

24 MR. MARSHALL: The plaintiffs are only alleging  
25 that they have a fear that the hackers may do so.

26 But, there is no allegation that the hackers

## Proceedings

1  
2 themselves published anything.

3 THE COURT: That is getting into real subtleties.

4 Because, I look at it as a Pandora's box. Once it  
5 is opened it doesn't matter who does what with it. It is  
6 out there. It is out there in the world, that information.

7 And whether or not it's actually used later on to  
8 get any benefit by the hackers, that in my mind is not the  
9 issue. The issue is that it was in their vault.

10 Let's just say to visualize this, the information  
11 was in Sony's vault. Somebody opened it up. It is now,  
12 this comes out of the vault. But, whether or not it's  
13 actually used that is something, that's separate.

14 On the one hand it is locked down and sealed. But,  
15 now you have opened it up.

16 You cannot ignore the fact that it's opened for  
17 everyone to look at.

18 So, that in the sense, that is why I had the  
19 discussion with counsel about publication versus disclosure.  
20 Publication is just getting it out there. Whether or not if  
21 this were in the box, still there is no publication.

22 When you open up the box, it's The Pandora's box.  
23 Everything comes out.

24 MR. MARSHALL: But, the information was stolen.

25 THE COURT: I know the information was stolen.

26 But, the way I look at it the information was

## Proceedings

1  
2 stolen, so that in itself is something that is out of the  
3 box. It is no longer in the box.

4 MR. MARSHALL: There is a New York case that tells  
5 you what publication is.

6 THE COURT: With a data breach situation?

7 MR. MARSHALL: Very similar. A hacking situation.

8 THE COURT: What is the case?

9 MR. MARSHALL: It was in our brief, Lunney versus  
10 Broad Prodigy Services Company.

11 THE COURT: Hold on a second. I think I might have  
12 it.

13 MR. De NATALE: Do you have a copy, counsel?

14 MR. MARSHALL: It is in our brief.

15 THE COURT: Hold on a second.

16 (Peruses)

17 THE COURT: You have got to like the decision when  
18 it starts out by saying, some infantile practical joker.  
19 You have got to like that.

20 (Peruses)

21 THE COURT: It says right here, the plaintiff now  
22 seeks monetary damages as compensation for the emotional  
23 distress which I consequently suffered not from the  
24 originator of this low brow practical joke, but instead from  
25 The Prodigy Services Company, hereinafter, Prodigy. The  
26 company which in effect furnished the medium through which



## Proceedings

the offensive message was sent.

That's not the case here. That is not a hacking case.

MR. MARSHALL: Someone broke into Prodigy's system, created a fictional e-mail account and then transmitted obscene e-mails and put them on the bulletin board.

It's very similar.

THE COURT: That's breaking into or that's hacking into a system to send a message.

This is different. This is hacking into a system and getting information out.

One is using that system to transmit. The other, in my case here, is breaking into a system to get information.

This is not a getting information. This is giving information.

MR. MARSHALL: Well, if anything is publication it would have been hacking in hand, then transmitting information out to the public, which is Prodigy. Right?

That's more close to publication than stealing information.

THE COURT: No. That I would tend to agree The Court seeing that may not be a -- you're hacking into a system to get information out. That's less likely.

That's very different from my situation where, you

## Proceedings

1  
2 know, I've got something locked down in a box and sealed, at  
3 least I believe it is, for no one to get into. And all of a  
4 sudden someone pops it out and this just gets out.

5 Those are apples and oranges types of facts here.  
6 I'm not so sure I'm agreeing with that argument.

7 But, I think Mr. Coughlin wants to respond now.

8 MR. COUGHLIN: I've been waiting patiently.

9 Your Honor, I want to start with a comment that my  
10 adversary made when he was arguing about the clause in this  
11 definition. And he called it an exclusion.

12 It is not an exclusion.

13 THE COURT: No, it is not.

14 MR. COUGHLIN: It is what I would characterize as a  
15 gate keeper issue.

16 It is part of the insurance grant which Sony has  
17 the burden to satisfy.

18 THE COURT: It's a coverage portion.

19 MR. COUGHLIN: It is the insuring grant. You're  
20 absolutely right.

21 THE COURT: I'm not disputing that.

22 MR. COUGHLIN: Let's look at the history of this.

23 In their opening brief Sony says there was a  
24 publication.

25 And I refer you to a couple of words and a couple  
26 of the 50 odd class actions which have that word.

## Proceedings

1  
2 But, at the same time they were arguing in the  
3 consolidated class action that we didn't do anything wrong.  
4 We didn't disclose anything. We didn't publish anything.  
5 We did nothing. We are a victim, as your Honor has  
6 characterized this.

7 And they cited for The Court a number of cases  
8 which have dealt with that clause and the oral or written  
9 publication issue.

10 Every one of those cases that they cited to you  
11 included a finding by The Court that there was a necessary  
12 and affirmative act by the insured.

13 And the reason that's important, Judge, and I want  
14 to get --

15 THE COURT: That's all of the pollution cases.

16 MR. COUGHLIN: No, Judge. That has nothing to do  
17 with this point right here.

18 My adversary talked about slips and falls, and  
19 bodily injury and all of the rest of that.

20 Third party liability is addressed in part A of a  
21 general liability policy. And it protects an insured for  
22 3rd party negligence and injury.

23 However, the personal injury section has specific  
24 enumerated torts which all have intention as part of their  
25 requirements.

26 And although Sony would like to ignore The County

## Proceedings

1  
2 of Columbia case, The Court of Appeals in that decision said  
3 you have to have intentional affirmative conduct by the  
4 insured here.

5 THE COURT: I know in that Columbia County case it  
6 has to do with a pollution case.

7 MR. COUGHLIN: But, The Court went on, Judge,  
8 though. The facts of that case dealt with seepage of  
9 pollution.

10 But, in that opinion The Court made it clear in  
11 their discussion of the personal injury section of the  
12 policy the view, which is the national view, that there must  
13 be affirmative conduct, action by the policyholder for that  
14 to kick in.

15 THE COURT: There we are talking about 14C;  
16 correct?

17 MR. COUGHLIN: No, Judge. With all due respect,  
18 they went beyond that.

19 Sony would like you to believe that that is all  
20 they did.

21 But, The Court, and I refer you to page 628. And  
22 they are talking about D.

23 THE COURT: Page 628? Hold on a second.

24 Got it.

25 MR. COUGHLIN: It is the last page of the decision,  
26 your Honor.

## Proceedings

THE COURT: Yes.

MR. COUGHLIN: Evidence that only purposeful acts acting were to fall within the purview of the personal injury endorsement is provided in part by examining the types of torts, plural, enumerated in the endorsement in addition to wrongful entry/eviction and invasion.

And then they go on to say, false arrest, detention, imprisonment, malicious prosecution, defamation and invasion of privacy by publication.

Read, and I'm quoting, "Read in the context of these other enumerated torts the provision here could not have been intended to cover the kind of indirect and incremental harm that results from property injury from pollution."

The importance of that clause, Judge, to this case is significant.

And Judge, the other part that I think is very important is the total shift --

Would you like me to wait, Judge?

THE COURT: Yes. Give me a second. I'm just looking at something.

(Peruses)

THE COURT: Here's the question I have for you on that Columbia case.

It says here, we agree with The Appellate Division

Proceedings

that coverage under the personal injury endorsement provision in question was intended to reach only purposeful actions undertaken by the insured or its agents.

Then, this goes on to say, evidence that only purposeful acts were to fall within the purview of the personal injury endorsement provided, in fact, by examining the types of torts enumerated in the endorsement in addition to wrongful injury, eviction, invasion, false arrest, detention, and malicious prosecution, defamation and invasion of privacy by publication.

In the context of these other enumerated torts the provisions could not be intended to cover the kind of indirect nor incremental harm that results from property injury from pollution.

I looked at that. And that's what I said earlier. I mentioned this to counsel earlier.

There is case law that lumps A through E together. Right? It's a policyholder.

The only way you're going to get coverage or the only way this is coverage, the policyholder has to commit these acts under A through E.

MR. COUGHLIN: Respectfully, they don't lump them together, Judge.

This is such a unique grant of coverage. They separated out.

## Proceedings

1  
2 THE COURT: But, they ultimately say, it's the  
3 policyholder that has to do it; right?

4 MR. COUGHLIN: There is no question. The Court of  
5 Appeals is in a main stream on that.

6 THE COURT: Here's the question I have for you.

7 Looking at that, F and G, that we have here now,  
8 they didn't talk about. But, we have that F and G here now.

9 Counsel is saying that at some point there was some  
10 shifting of the policy, some sort of changing. But, in any  
11 case, F and G is in here in this definition section. Okay.

12 All right. So, F says "The use of another's  
13 advertising idea in your advertisement." That's in quotes.  
14 Or G, "Infringing upon another's copyright, trade, dress or  
15 slogan in your advertisement." And that's in quotes.

16 So, I thought, okay. What does advertisement mean?

17 So, you go back to the beginning of advertisement.  
18 And where it says in advertisement, it's very interesting  
19 what it says in section 5, 1. Advertisement, in quotes,  
20 "Means a notice that is broadcast or published to the  
21 general public or specific market segment about your goods,  
22 products or services for the purpose of attracting customers  
23 or supporters for the purpose of this definition."

24 A, notices in a publication include material placed  
25 on the internet or similar electronic means for  
26 communication.

## Proceedings

1  
2 And B, regarding the web sites, only that part of  
3 the web site that is about your goods, products or services  
4 for the purposes of attracting customers or supporters is  
5 considered an advertisement.

6 When I looked at that definition of advertisement,  
7 that doesn't say anywhere that it says by the policyholder.  
8 That says, generally speaking.

9 I mean, not even generally speaking. It says,  
10 advertisement. It doesn't say that you, the policyholder.

11 MR. COUGHLIN: You have got to go back to the  
12 start. The personal injury section talks about the  
13 insured's business.

14 This has nothing to do with this case, Judge,  
15 nothing.

16 THE COURT: That has a lot to do with the case.  
17 Because, I'm trying to figure out whether or not E, that is  
18 at issue here, requires that it has to be committed by the  
19 policyholder or it can be read the way it is written to  
20 include not only the policy holder's acts but other people's  
21 acts.

22 MR. COUGHLIN: With all due respect, it is not  
23 written that way.

24 And The Court of Appeals, which is governing law,  
25 recognized that it has to be an affirmative act.

26 THE COURT: I understand that. But, The Court of



## Proceedings

1 Appeals did not have F and G in front of it.

2 MR. COUGHLIN: Judge, you don't have F and G in  
3 front of you.

4 It is not, respectfully, it is not an issue in that  
5 case.

6 THE COURT: You know, when I make this an issue  
7 this becomes an issue.

8 That's what I have in front of me.

9 Look, it is not Orwellian where I can say it  
10 doesn't exist, and I'm not going to look at it and I'm just  
11 going to limit myself to what you put in front of me.

12 I'm an educated fellow, I can read everything.

13 I cannot look at these policy provisions in a  
14 vacuum and say this is what it is, I don't care what the  
15 other clause says. That is not how you read policies.

16 MR. COUGHLIN: Judge, Sony is invoking coverage  
17 through the oral or written publication clause.

18 THE COURT: Right. And the fight between you two  
19 now is that you are saying that E means it has to be conduct  
20 by, has to be perpetrated or performed by a policyholder.

21 They are arguing saying, no, that is not how it is  
22 read. It can include not just us but other actions or acts  
23 by other people.

24 That's what the fight is.

25 MR. COUGHLIN: Well, truthfully, Judge, they are  
26

## Proceedings

arguing both.

In their opening brief they argue they satisfied the publication requirement. Because, they pulled a couple of words out and they cited a whole bunch of cases to you.

All of them require, however, purposeful conduct.

THE COURT: I'm not so sure I agree with them saying that they are the publication. That they published it. Okay. That is one aspect.

MR. COUGHLIN: That is part one.

In the reply they shifted gears completely.

To satisfy their burden they are now saying, ignore the oral or written publication issue. Replace the word publication with disclosure of personal information.

And your Honor brought up the "in any manner."

In any manner is a clause that affects the publication issue. It is not disclosure of personal information in any manner. It doesn't modify that phrase. It modifies the prior one just on sentence construction.

But, the idea, and this goes back to some comments your Honor made on the exclusion section, the idea that you can ignore words in a contract and say we are going to ignore the oral or written phrase, we're going to white it out. We don't like the idea of publication. So, we are going to call it disclosure now. And we are going to read just disclosure of personal information, which could be by

## Proceedings

anybody anywhere, that is not what this coverage provides.

And the words negligent disclosure, that is not on this part of the policy, your Honor.

But, everybody knows there is no coverage under part A of the policy.

THE COURT: The thing I look at in terms of the County of Columbia case, they don't use the wording in any manner anywhere in their description. So, I don't know if they had that issue in front of them with the phrase, in any manner. That's number one.

Number two, with respect to the coverage provision in A, under A for bodily injury and property injury, there is no personal and advertising injury in there. Right?

MR. COUGHLIN: Judge, that's not a part of the case. They acknowledge.

THE COURT: I know. But, you brought it to my attention.

MR. COUGHLIN: I didn't. They did.

THE COURT: Okay. Whoever brought it to my attention, it is not there.

So, I'm only focusing on the coverage B.

MR. COUGHLIN: Correct.

THE COURT: I'm not so sure that in any manner can be just read the way you're reading this.

Why would you put in any manner? If you wanted to

## Proceedings

1  
2 keep it simple and not even make this more complicated than  
3 it is? You could have just left it alone and done what the  
4 West Virginia court did and just have it like that without  
5 using "in any manner."

6 Why all of a sudden? How can I ignore in any  
7 manner?

8 MR. COUGHLIN: You don't need to ignore this,  
9 Judge. You put this where it belongs.

10 THE COURT: Wait a minute. When you say where it  
11 belongs, I'm not putting this anywhere. I'm just reading it  
12 the way it is here.

13 It says oral or written publication in any manner  
14 of material that violates a person's right of privacy.

15 MR. COUGHLIN: Correct. Oral or written  
16 publication in any manner.

17 THE COURT: So, what does that mean to you?

18 MR. COUGHLIN: This means that there are many ways  
19 to publicize it. An oral or written publication in any way.

20 It doesn't mean you can replace the word  
21 publication with disclosure. And it doesn't mean --

22 THE COURT: I agree with you. That's fine.

23 MR. COUGHLIN: Well, they cannot get beyond that  
24 issue, your Honor.

25 But, also, you don't apply it the way the sentence  
26 structure is drafted to the disclosure of personal

## Proceedings

1  
2 information. It does not apply there. It applies to the  
3 prior clause.

4 And I think it's clear there.

5 And there are cases, Judge, around the country.  
6 And there are a handful of them. Every one of those cases  
7 recognized they had to find a publication that was caused by  
8 the policyholder. And there are like 7 or 8.

9 In their opening brief they cite a bunch. We cite  
10 many of them for the same proposition.

11 THE COURT: Those publications had to do with  
12 defamation, though, right?

13 MR. COUGHLIN: No. These are data disclosure  
14 cases, Judge. All of them, every one of them is data  
15 disclosure case.

16 Judge, can I just point out a case that I think  
17 answers your question from The Federal Circuit, The 11th  
18 Circuit?

19 THE COURT: These are all cases outside of state,  
20 though. Therefore, not guidance in the sense that I can  
21 look at to see where I want to go with them.

22 MR. COUGHLIN: Correct, Judge. But, I was  
23 answering your direct question.

24 In our brief we point out that in the Creative  
25 Hospitality Ventures case The Court ruled the phrase, in any  
26 manner, merely expands the category of publications such as

## Proceedings

1  
2 e-mails, handwritten letters and perhaps blast factors  
3 covered by the policy.

4 THE COURT: What is the cite of the case? What is  
5 the name of the case?

6 MR. COUGHLIN: I am sorry. It's Creative  
7 Hospitality Ventures versus US Liability Insurance Company.

8 THE COURT: Do you have a copy? I don't have that.

9 MR. COUGHLIN: I don't have it with me, your Honor.

10 MR. MARSHALL: Yes, your Honor.

11 We are going to pull out the whole case.

12 THE COURT: A piece meal of it. Okay.

13 MR. MARSHALL: Yes. Cited in our brief, your  
14 Honor.

15 (Handed)

16 THE COURT: I am not sure I understand what they are  
17 trying to say.

18 "We likewise reject the ETL argument that the  
19 phrase in any manner expands the definition of publication  
20 to include the provision of a written receipt."

21 And then they go on to say, The District Court  
22 noted the phrase "in my manner" merely expands the  
23 categories of publications such as e-mails, handwritten  
24 letters and perhaps blast factors covered by the policy.  
25 But, the phrase cannot change the plain meaning of the  
26 underlying terms of publication.

## Proceedings

1 So, why isn't a written receipt a publication?

2 I mean, it looks like an inconsistency there.

3 MR. COUGHLIN: No. Because, they took the written  
4 receipt as being a disclosure from the, I believe it was  
5 that cash register backed out into the public to the person  
6 who gave the credit card.

7 THE COURT: Okay.

8 An argument is, the way this is set up, an oral or  
9 written publication in any manner is the medium in terms of  
10 how that's being transmitted.

11 MR. COUGHLIN: Yes. We view that's how that has to  
12 be read.

13 The problem, Judge, is the theory that Sony is  
14 urging you to adopt requires you to take out the oral or  
15 written publication part of the enumerated defense and just  
16 put in the word disclosure in any manner of personal  
17 information. Which is, by the way, in that case, absolutely  
18 applies to the hackers.

19 And that is not what this coverage was intended to  
20 do.

21 And The Court of Appeals, I know they don't like  
22 the case, but The Court of Appeals made it clear what their  
23 version of the personal injury protection or coverage grant  
24 is, Judge.

25 And it is so special, Judge. Because, it is so  
26

## Proceedings

different than the 3rd party liability cases.

Your Honor brought up the construction defect cases, which as we all know New York County is a unique animal in that litigation in the country.

But, those cases, Judge, and the AI issues between the subs and the generals and the owners, etc, they all stay in part A. And they have absolutely no applicability to this problem.

This is a limited grant of coverage by definition, which is what The Court in County of Columbia was saying.

And your Honor, it is consistent with the cases nationally, the cases on the data breach issue and the violation issues that are springing up around the country, every one of them.

And I'm saying 100 percent of them have required an affirmative act by the policyholder and a publication. Every one of them.

That's why, Judge, Sony flipped in their reply and said, we are getting away from the publication issue. Forget it. We said that, no, we are going to go only at the disclosure of personal information issue.

And by the way, Judge, they don't cite one case in support of that issue, because there isn't one out there.

This is a gate keeper issue. This is one that they cannot get into the coverage without satisfying.



## Proceedings

1  
2 And as The Court of Appeals said over and over  
3 again, in insurance contracts you have to apply all the  
4 terms.

5 The only way they get here is to replace the terms.

6 THE COURT: Okay. Let me ask Mitsui one question.

7 Why did you add data breach exclusion after the  
8 fact if you believed this wasn't covered in this language?

9 MR. MARSHALL: We would never have expected to even  
10 be in this litigation.

11 I mean, to equate publication with the theft of  
12 information is such an extraordinary expansion of the policy  
13 that one would never even contemplate that we would be in  
14 this battle.

15 There was no, it didn't alter the premium. We  
16 didn't pull any coverage. There was no carve-out in the  
17 exclusion. It was simply meant to clarify the intent of the  
18 policy.

19 But, that policy is not at issue here. The policy  
20 at issue says oral or written publication.

21 And I need to pose a rhetorical question. That is,  
22 what is the oral or written publication?

23 MR. De NATALE: May I respond, your Honor?

24 THE COURT: I'll give you a minute.

25 MR. MARSHALL: I pose that rhetorical question  
26 because the argument has been the language or the phrase,

## Proceedings

"in any manner," somehow expands it to the notion of the theft of information or inadequate security.

But, the only court in the country that squarely addresses the "in any manner" language is The 11th Circuit in the Creative Hospitality case. That is the only case in the country.

And they say, and quite clearly and I think quite logically, that the "in any manner" language is meant to go to like you said, the media of the publication. It doesn't weed out the publication.

Furthermore, your Honor mentioned the advertising injury cases as support for the proposition that, hey, there may be situations here where it doesn't require conduct by the policyholder. Well, the case law does not say that.

And in our brief on page 24 we direct your Honor to case law addressing that. Micon Sales Incorporated versus Diamond State Insurance Company, which cited to the reported California decision.

This involved the lawsuit against the insured for manufacturing clothing wrongfully bearing the plaintiff's trademark and against a retailer for advertising and selling the infringed clothing.

The insured argued that the claim implicated advertising coverage on the basis that it reasonably could have expected coverage to the extent of advertising

## Proceedings

activities of others even though there was no allegation that the insured engaged in advertising activity.

The Court rejected that. The Court said that construing provisions to the acts of the 3rd party who was not privy to the contract cannot be considered an obviously reasonable expectation.

And in denying coverage The Court found the liability insurance purchase to protect against actions of the insured, not remote 3rd parties.

So, also, in the advertising injury context the courts have ruled this requires affirmative conduct by the insured, which we do not have here.

Moreover, every case that SCA cites in support of their position, every case they cite in support of their provision that has to do with the invasion of privacy involved the affirmative purposeful transmittal of material by the party against whom liability is asserted.

THE COURT: You know --

MR. MARSHALL: Affirmative purposeful transmittal of information.

THE COURT: You know, the oral and written publication in any manner phrase, I understand what the defense counsel -- I mean, plaintiff's counsel is arguing.

Well, before I say anything, why don't you tell me your response.

## Proceedings

1  
2 MR. De NATALE: If I may, your Honor. I'm glad  
3 your Honor mentioned the exclusion in the next Mitsui  
4 policy, the 2012 policy.

5 It shows that insurers knew how to exclude risk  
6 when they want to. When they want to exclude things they  
7 do. And that is what they did after the data breach.

8 What I hear here is that we are struggling mightily  
9 to put words in the policy that just aren't there.

10 The policy doesn't say it has to be by the  
11 policyholder.

12 THE COURT: The point that I'm hearing very clearly  
13 is that oral written publication in any manner, it talks  
14 about the medium in getting the case that discusses that.

15 MR. De NATALE: I see that case and that's not what  
16 it says.

17 Your Honor says correctly that would create a  
18 pollution in saying that it is saying that in any manner  
19 means in any media.

20 They could have written that. They could have said  
21 oral or written publication in any media.

22 It says, in any manner.

23 When I read in any manner this sounds to me whether  
24 this be negligent or intentional.

25 It says publication in any manner. To me that says  
26 whether this be by the policy holder or whether the policy

## Proceedings

holder's negligence allows someone else to make the publication.

THE COURT: That's interesting that you make that point.

That First Department case where they make this distinction in that construction case where it had to do with acts and omission versus negligent acts and omission, they did not, The First Department held they didn't use the word negligent acting and omissions. Therefore, it is only merely acts and omissions that count that determines whether or not there is coverage.

That drops it down to a lower threshold. Because, when you talk about negligent acting and omissions you would have to go through all of the breach of duty and proximate cause.

If you just drop it down to just merely acts and omission that's a simpler thing to get over. Whether there was an act or omission that the trier of facts has to find to trigger coverage.

That's interesting. This doesn't say negligent or intentional. It just says in any manner.

MR. De NATALE: The County of Columbia case, I think the insurers are putting too much weight on that case.

THE COURT: But, the problem with that is that this entire policy it talks about, it's very policyholder

## Proceedings

oriented.

Everything talks about the policyholder has to do this, the insured has to do that; this, that.

Now, we get down to this one area here where you are saying, no, that does not mean insured only. It means anybody.

So that you're asking me in that sense now to carve-out this little island for you saying, well, in this one particular -- never mind what you read throughout this entire policy which just says insured, insured, insured, here. And there are also provisions later on talking about third party acts.

But, when you get to this anything provision here, and I was pointing out F and G and how there was a dichotomy there and there might be a problem. When you point to E you say that has to be treated differently, like the tail wagging the dog.

MR. De NATALE: We are not.

These policies cover a policy hold. When you buy insurance it's the claim made against you. If you are sued for these kinds of offenses you're covered.

And you can be sued as a principal, as a respondent. You can be sued because you allowed someone else to do something.

If the claim against you is for defamation, or for

## Proceedings

1  
2 privacy or for copyright infringement, you can negligently  
3 infringe on somebody's copyright.

4 It's the claim against you that is covered , not  
5 necessarily your own conduct.

6 You can be liable for a claim, you're entitled to a  
7 defense.

8 THE COURT: Mr. Coughlin, isn't the medium to be  
9 arguably the hackers themselves or the medium that  
10 transmitted or publicized all of this information?

11 MR. COUGHLIN: No. Because, it is the manner in  
12 which the policyholder and its affirmative act published the  
13 information. That is the difference here, Judge.

14 The hackers, the criminals have no tie to Sony.

15 So, no. It cannot fit within that shoehorn.

16 THE COURT: Where does it say it has to be tied to  
17 Sony? Where does it say that the publication --

18 MR. COUGHLIN: The oral or written publication by  
19 every interpretation deals with the specific affirmative act  
20 by the policyholder.

21 Every one, every court in the country that has  
22 dealt with it, your Honor, has found that.

23 MR. De NATALE: That is not true.

24 MR. COUGHLIN: Excuse me. May I have the floor?

25 THE COURT: Hold on. You guys didn't hear what I  
26 said. You will get your opportunity.

## Proceedings

1  
2 MR. COUGHLIN: Your Honor, the oral or written  
3 publication goes to an enumerated tort under the personal  
4 injury coverage.

5 Every court that has looked at it says that the  
6 oral or written publication has to be by the policyholder.  
7 Every one of them. There is no exception.

8 THE COURT: But, those courts on a large scale data  
9 breach as this would say the same thing?

10 Is that what you're arguing?

11 MR. COUGHLIN: Absolutely.

12 We know now, Judge, that this case has been  
13 seriously de-risked.

14 That's not an issue. It is not relevant to the  
15 coverage issue. It's not relevant at all, respectfully.  
16 The disclosure --

17 And by the way, Sony knows they have a real problem  
18 with the oral or written publication issue. Because, in  
19 their opening brief to you that was all over their brief.

20 And their justification was to pull out the word  
21 publication from a couple of the complaints and ignore New  
22 York law that says you look to the gravamen of the problem.

23 But, then they see our reply, our responsive brief  
24 where we even point out that every case they cited to you in  
25 support of their publication issue actually supports  
26 insurers.



## Proceedings

1  
2 So, in the reply, their response, they flipped.  
3 Completely put aside publication. We are not arguing that.  
4 We are now substituting disclosure, the word, and taking out  
5 oral or written publication. And they only want that phrase  
6 to read, disclosure of personal information.

7 MR. MARSHALL: I have an answer for your Honor to  
8 your question.

9 THE COURT: What is that?

10 MR. MARSHALL: That is, The Court has addressed a  
11 data breach of this magnitude.

12 THE COURT: Yes?

13 MR. MARSHALL: It's an unpublished decision from  
14 Connecticut. It is called, Recall Total Information  
15 Management versus Fed Insurance Company, 2012 Westlaw,  
16 469988.

17 And in that case a cart containing electronic media  
18 fell out of a transport van near a highway. So, it was  
19 under the control of the insured that it fell out of the  
20 van.

21 The cart and, approximately, 130 computer data  
22 tapes containing personal information for more than 500,000  
23 IBM employees were then removed by an unknown person and  
24 never recovered.

25 The insured was then sued for that negligence.

26 And in that case The Court found that there was no

## Proceedings

publication.

So, that is a data breach of the magnitude we are dealing with here.

And I think it's very important to understand that every case cited by Sony in support of the proposition that negligent security can be equated with publication, again, involved affirmative conduct by the insured. Every one of their cases.

And if this Court were to hold that these underlying data breach claims implicate the oral or written publication offense you would, essentially, weed out the first phrase of that offense. It would become meaningless.

Because, if that is covered then somebody that breaks into this courthouse and steals the confidential pleadings filed in this case, if that occurred then this court would be deemed to have published the information.

That is what we are dealing with here. We are dealing with the theft of information.

Moreover, the hackers themselves aren't alleged to have published. There is no oral or written publication.

MR. De NATALE: Your Honor, if I may?

Counsel keeps saying things that are just not right.

You have to address them. There are cases from around the country that have found that in situations of

## Proceedings

1  
2 passive access to information or inadvertent access to  
3 information can be a publication within the meaning of that  
4 policy case.

5 The Barrier (phonetics) case from West Virginia, a  
6 hotel installed surveillance cameras to a certain part of  
7 the hotel that could be accessed from the manager's office.

8 THE COURT: That was all of the policyholders.

9 MR. De NATALE: But, hear me out.

10 The Court said, installing the cameras was a  
11 violation. But, also the fact that there were people who  
12 could inadvertently see those clients and see the  
13 recordings, that was a publication.

14 THE COURT: The primary actor in the case was the  
15 policy holder?

16 MR. De NATALE: I think we are parsing this too  
17 fine.

18 In the NWN case from Oklahoma, the company had baby  
19 monitors installed in confidential counseling sessions. And  
20 the court found that the fact that that could be overheard  
21 by other people in the waiting room accessed, being  
22 overheard, that kind of passive access amounted to a  
23 publication.

24 THE COURT: The publication, you know, the issue I  
25 don't think it's that difficult here.

26 But, the question that I have, the hard question

## Proceedings

that counsel keeps driving home you cannot get around.

His argument is, if I were to find that E allows for coverage for 3rd party acts, the hackers, I would be essentially rewriting this contract, the insurance contract. And expanding liabilities that they said that the coverage, expanding coverage when it was never contemplated.

MR. De NATALE: With all due respect, I think the after the fact argument --

The Lens Crafter's case from California, the matter personally involved, one of the issues in the Lens Crafter's case was when you went into Lens Crafter's and had your eyes examined.

THE COURT: Hold on a second.

(Short pause)

THE COURT: Go ahead.

MR. De NATALE: One of the issues in the Lens Crafter's case was when you went into Lens Crafter's and gave your eye exam to your optometrist there was another person sitting in the room who was not authorized to be there. That person didn't do anything but listen. That person heard you disclose your confidential information and had unauthorized access to that confidential information.

That was deemed to be a publication within the meaning of the privacy law.

It's a situation where passive access is not an

## Proceedings

1 affirmative act. The only person speaking is the patient.

2 But, the passive access by the unauthorized person  
3 gave rise to a claim that it was covered under the privacy  
4 clause.

5 THE COURT: The Court said there was coverage.

6 That's a situation where they were inside Lens  
7 Crafter's and Lens Crafter's themselves let someone  
8 unauthorized sit in that room.

9 You know, we are getting really far away from the  
10 actual facts in the case that I have versus the facts in  
11 your case.

12 I mean, that is not a situation where you got the  
13 information, the patient's information and then someone on  
14 the outside is hacking into the Lens Crafter's computer  
15 system and taking all of that information.

16 MR. De NATALE: I'm saying, these are cases of  
17 passive access not purposeful by the policyholder.

18 There is no case on point either way. There is not  
19 a single case that says a massive data breach.

20 If I could make one other point.

21 In a duty to defend case, this isn't ultimate  
22 coverage.

23 Your Honor is well aware of how broad the duty to  
24 defend is.

25 I hear a struggling mightily to read words into the  
26

## Proceedings

1  
2 policy that aren't there.

3 Committed by the policyholder, section C says that.  
4 Section G does not say that.

5 And we are looking at the underlying complaints and  
6 they are saying, yes, it says publication.

7 We have been sued in underlying cases for invasion  
8 of privacy, violation of privacy rights, disclosing  
9 confidential information. And I don't think we have to work  
10 that hard to establish that we are entitled to a defense  
11 absent some clear language.

12 THE COURT: But, it is your burden when you have to  
13 decide coverage.

14 MR. De NATALE: But, the policy has to be read  
15 broadly. That's their burden.

16 THE COURT: Mitsui made a good point. What is the  
17 oral written aspect of this publication?

18 MR. De NATALE: The publication here is that the  
19 information was reviewed due to Sony's alleged negligence.

20 THE COURT: What was oral or written about this?

21 MR. De NATALE: Oral or written includes  
22 electronics. That's absolutely clear.

23 The insurer cannot contest that. And their policy  
24 says that.

25 The publication was the hacking, taking and copying  
26 and potentially putting on the cyber black market the

## Proceedings

information of millions and millions of customers.

They are taking that from Sony. That's a release of information, disclosure of information, an inadvertent publication of private information of millions of customers.

The policy says publication in any manner. And when someone else gets into your system and releases information into the internet, that's a publication.

And in the absence of clear language in the policy that excludes that kind of act we have coverage. And we have a defense.

MR. MARSHALL: With all due respect, your Honor, we are not trying to read into the policy exclusions that don't exist. We are asking --

THE COURT: We are trying to figure out coverage.

Let's get the terms correct here. The terms are not interchangeable.

This is all strictly a coverage issue here that I have to figure out whether or not I'm going to agree with the plaintiff Zurich or the defendant Sony with respect to this coverage issue.

MR. MARSHALL: Yes.

THE COURT: That is the bottom line.

MR. MARSHALL: And the bottom line is that we are asking The Court to preserve the language as written.

We are asking The Court to not gloss over the oral

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

Proceedings

or written publication language.

This would be a very different case, and I would admit this would be a very different case had Sony negligently posted personal information on line which was then accessible to third parties. It would be a totally different case.

But, that's not what happened here.

What happened here was information was stolen.

And to equate publication with the theft of information is to essentially say, I'm going to ignore the word publication. Because, no definition of publication includes theft.

THE COURT: Okay. Mr. Coughlin, your response?

MR. COUGHLIN: I have nothing further, your Honor.

Thank you for your time.

THE COURT: All right. I have heard the argument. I'm giving you a decision and order right now. Because, I think it's important enough that it needs to seek Appellate review as quickly as possible.

You know, there is that struggle here with respect to paragraph E here, 14E, oral or written publication in any manner of material that violates a person's right of privacy.

It is clear that the courts have passed on portions of this type of coverage here and required that the



## Proceedings

1  
2 coverage, for coverage to actually get triggered it would  
3 have to be, the acts have to be conducted or perpetrated by  
4 the policyholder.

5 What I'm being asked now, and the cases are clear  
6 about that, the policyholder has to act. And it's very  
7 limited circumstances.

8 The West Virginia court is one of them.

9 The Butts case has limited the instance where it  
10 says it would be a 3rd party with respect to the  
11 dissemination or publication of slanderous material. That's  
12 the case where they took a little bit of a twist there.

13 But, at the bottom here, the bottom line is the  
14 question of whether or not paragraph E requires, or at least  
15 coverage is only available when it is performed or done,  
16 undertaken by the policyholder or the policyholder's  
17 affiliates and employees and so forth.

18 In this case here I have a situation where we have  
19 a hacking, an illegal intrusion into the defendant Sony's  
20 secured sites where they had all of the information.

21 That information is there. It's supposed to be  
22 safeguarded. That is the agreement that they had with the  
23 consumers that partake or participated in that system.

24 So that in the box it is safe and it is secured.  
25 Once it is opened, it comes out.

26 And this is where I believe that's where the

## Proceedings

1  
2 publication comes in. It's been opened. It comes out. It  
3 doesn't matter if it has to be oral or written.

4 We are talking about the internet now. We are  
5 talking about the electronic age that we live in. So that  
6 in itself, by just merely opening up that safeguard or that  
7 safe box where all of the information was, in my mind my  
8 finding is that that is publication. It's done.

9 The question now becomes, was that a publication  
10 that was perpetrated by Sony or was that done by the  
11 hackers.

12 There is no way I can find that Sony did that.

13 As Mitsui's counsel said, this would have been a  
14 totally different case if Sony negligently opened the box  
15 and let all of that information out. I don't think we would  
16 be here today if that were the case.

17 This is a case where Sony tried or continued to  
18 maintain security for this information. It was to no avail.  
19 Hackers got in, criminally got in. They opened it up and  
20 they took the information.

21 So, the question then becomes is that something of  
22 the kind that is an oral or written publication in any  
23 manner.

24 You know, I heard the arguments going back and  
25 forth.

26 I am not convinced that that is oral or written

## Proceedings

publication in any manner done by Sony.

That is an oral or written publication that was perpetrated by the hackers.

In any manner, as Zurich's counsel pointed out, means oral or written publication in any manner. It is the medium. It is the kind of way it is being publicized. It's either by fax, it is either by e-mail, either by so forth. But, it doesn't define who actually sends that kind of publication.

And in this case it is without doubt in my mind, my finding is the hackers did this.

The 3rd party hackers took it. They breached the security. They have gotten through all of the security levels and they were able to get access to this.

That is not the same as saying Sony did this.

But, when I read E, E can only be in my mind read that it requires the policyholder to perpetrate or commit the act.

It does not expand. It cannot be expanded to include 3rd party acts.

As we are going back and forth, back and forth, the policy could be read this way and that way, the bottom line is it is written the way it is written.

And my finding is when you read oral or written publication in my manner, that talks about the kind of way

## Proceedings

that it is sent out there and disseminated in the world.

It doesn't talk about who is actually doing that dissemination for that sort of a publication.

In my mind that does not alter the policy language here that covers an insured policyholder for their acts or for their negligence and so forth.

I cannot help but think that if you look at the entire policy, when I focus on this area here, paragraph E, that that has to take a different approach. That now, all of a sudden, the policy in general takes a different approach and includes acts by 3rd parties.

That's not what this says. It is just not what this says. And I cannot read it to say that.

And if I were to read it to include that , that would run into what we had discussed or argued earlier. That would be expanding coverage beyond what the insurance carriers were entering into or knowingly entering into.

That's not an expansion of coverage that I'm willing to permit under the language, of the clear language that we have here.

They had to go back and forth. But, I cannot read this in any other way than that this requires the policy holders to act. Okay.

So, under these circumstances my finding, as I said earlier, is that paragraph E that is at issue in that case

## Proceedings

1  
2 requires coverage or provides coverage only in that  
3 situation where the defendants, Sony, SCA or SCEA, commits  
4 or perpetrates the act of publicizing the information.

5 In this case, they didn't do that. This was done  
6 by hackers, as I said.

7 And that is my decision and order.

8 The declaration is that there is no coverage under  
9 this policy for SCA or SCEA as a result of the hacking that  
10 was done with respect to the data breach in the underlying  
11 action.

12 So, that is, the motion, the motion for summary  
13 judgment by SCA, SCEA is denied.

14 The cross motion by Zurich and Mitsui is granted.

15 And the declaration is under paragraph E of this  
16 policy that I have in front of me today.

17 Paragraph E requires an act by or some kind of act  
18 or conduct by the policyholder in order for coverage to be  
19 present.

20 In this case my finding is that there was no act or  
21 conduct perpetrated by Sony, but it was done by 3rd party  
22 hackers illegally breaking into that security system. And  
23 that alone does not fall under paragraph E's coverage  
24 provision.

25 That's my decision and order.

26 So, I guess to finish that up there is no duty to

## Proceedings

defend by following that through.

Since this is something that is of a declaration, I am sufficient to have it the way it is set out here.

If you want to memorialize it and put it in a clearer language or order for me to sign, I'm happy to do that.

MR. COUGHLIN: Do you have a preference?

THE COURT: Why don't we leave it like this. Because, I think it is going to require immediate Appellate authority. So, you're Sony.

MR. COUGHLIN: I prevail. I will do the order.

THE COURT: You order the transcript. I will so order it. You will have it for your records.

I will put on the gray sheets that it is decided. I will put down that the motion is denied. Cross motion is granted. So, you will have an appealable order if you need to seek Appellate review right away. So, you don't have to wait for the transcript.

MR. MARSHALL: While we are on the record, may I ask Sony a question?

That is, given The Court's ruling and the fact that Mitsui moved on the same basis with respect to SOE and SNEI, does Sony wish to continue with this litigation and continue briefing that similar motion?

THE COURT: I'll answer for them.

## Proceedings

I think that that is something that you guys have to talk about outside of the courtroom. I won't put that on the record.

The dust will settle. You guys will have your work cut out for you in the next few weeks.

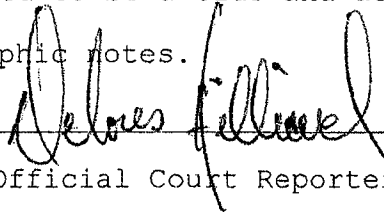
I'll let the dust settle on this.

Check with my part clerk to give you a control date as to where we are going to go with this. Okay?

Thank you. Have a good weekend.

\*\*\*

Certified to be a true and accurate transcription of said stenographic notes.

  
Official Court Reporter

3/3/14  
Index No. 651982/11  
mon seq no. 14  
So Ordered

  
JEFFREY K. OING  
J.S.C.

## **II.**

### **Coverage under Computer Fraud Policies**



25 N.Y.3d 675, 37 N.E.3d 78, 16  
N.Y.S.3d 21, 2015 N.Y. Slip Op. 05516

**\*\*1** Universal American Corp., Appellant  
v  
National Union Fire Insurance Company  
of Pittsburgh, Pa., Respondent.

Court of Appeals of New York  
Argued May 7, 2015  
Decided June 25, 2015

CITE TITLE AS: Universal Am. Corp. v  
National Union Fire Ins. Co. of Pittsburgh, Pa.

### SUMMARY

Appeal, by permission of the Court of Appeals, from an order of the Appellate Division of the Supreme Court in the First Judicial Department, entered October 1, 2013. The Appellate Division modified, on the law, an order of the Supreme Court, New York County (O. Peter Sherwood, J.; op 38 Misc 3d 859 [2013]), which had denied plaintiff's motion for partial summary judgment and granted defendant's cross motion for summary judgment dismissing the complaint. The modification consisted of declaring that the insurance policy does not provide coverage for the claimed loss. The Appellate Division affirmed the order as modified.

*Universal Am. Corp. v National Union Fire Ins. Co. of Pittsburgh, PA.*, 110 AD3d 434, affirmed.

### HEADNOTE

#### Insurance

#### Construction of Policy

Losses Caused by Fraudulent Entry of Electronic Data

The insuring agreement for computer systems fraud between plaintiff health insurance company and defendant insurer did not provide coverage for plaintiff's losses resulting from fraudulent health care claims paid through plaintiff's computer

system, because the agreement's application to "fraudulent . . . entry of Electronic Data or Computer Program" did not encompass losses caused by an authorized user's submission of fraudulent information into plaintiff's computer system. The test to determine whether an insurance contract is ambiguous focuses on the reasonable expectations of the average insured upon reading the policy and employing common speech. The agreement unambiguously applied to losses incurred from unauthorized access to plaintiff's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users. The term "fraudulent" refers to deceit and dishonesty and, in the agreement, qualified the act of entering or changing data or a computer program. The reference to "fraudulent" did not also qualify what was actually acted upon, namely the "electronic data" or "computer program" itself. The intentional word placement of "fraudulent" before "entry" and "change" manifested the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access.

### RESEARCH REFERENCES

Am Jur 2d, Computers and the Internet §§ 197, 239, 242, \*676 255; Am Jur 2d, Insurance §§ 289, 297–299, 503, 679, 1012, 1368, 1402, 1637, 1931, 2038.

Carmody-Wait 2d, Parties § 19:160; Carmody-Wait 2d, Summary Judgment §§ 39:12, 39:16.

Couch on Insurance (3d ed) §§ 21:14, 22:11, 22:14–22:15, 22:38, 126:30, 129:4, 131:33, 149:48, 201:18.

NY Jur 2d, Insurance §§ 818, 871, 1570–1571, 1626, 1636, 1686, 1697, 1703, 1740, 2018, 2082, 2321; NY Jur 2d, Telecommunications § 222.

### ANNOTATION REFERENCE

See ALR Index under Computers; Databases; Insurance; Fraud and Deceit.

## FIND SIMILAR CASES ON WESTLAW

Database: NY-ORCS

Query: insur! &amp; computer! /3 fraud!

## POINTS OF COUNSEL

*Schlam Stone & Dolan LLP*, New York City (Richard H. Dolan and Bradley J. Nash of counsel), for appellant.

I. The order below should be reversed, and partial summary judgment granted to Universal American Corp. on the issue of coverage. (*Executive Risk Indem., Inc. v Starwood Hotels & Resorts Worldwide, Inc.*, 98 AD3d 878; *Ace Wire & Cable Co. v Aetna Cas. & Sur. Co.*, 60 NY2d 390; *Belt Painting Corp. v TIG Ins. Co.*, 100 NY2d 377; *Dean v Tower Ins. Co. of N.Y.*, 19 NY3d 704; *Ragins v Hospitals Ins. Co., Inc.*, 22 NY3d 1019; *Westview Assoc. v Guaranty Natl. Ins. Co.*, 95 NY2d 334; *United States Fid. & Guar. Co. v Annunziata*, 67 NY2d 229; *City of New York v Evanston Ins. Co.*, 39 AD3d 153; *Primavera v Rose & Kiernan*, 248 AD2d 842; *Raner v Security Mut. Ins. Co.*, 102 AD3d 485.)

II. None of the exclusions to the computer fraud policy applies to Universal American Corp.'s claim. (*Dean v Tower Ins. Co. of N.Y.*, 84 AD3d 499, 19 NY3d 704; *Pioneer Tower Owners Assn. v State Farm Fire & Cas. Co.*, 12 NY3d 302; *Teichman v Community Hosp. of W. Suffolk*, 87 NY2d 514; *Belt Painting Corp. v TIG Ins. Co.*, 100 NY2d 377; *On Demand Mach. Corp. v Ingram Indus., Inc.*, 442 F3d 1331; *Commodity Trend Serv., Inc. v Commodity Futures Trading Commn.*, 233 F3d 981; *Kaminel Besicorp Allegany L.P. v Rochester Gas & Elec. Corp.*, 908 F Supp 1194; *MedAssets, Inc. v Federal Ins. Co.*, 705 F Supp 2d 1368; *Raner v Security Mut. Ins. Co.*, 102 AD3d 485; *Miller Tabak + Co., LLC v Senetek PLC*, 118 AD3d 520.)

\*677 *Nixon Peabody LLP*, New York City (Barbara A. Lukeman of counsel), for respondent.

I. The unanimous order of the First Department should be affirmed because Universal American Corp. cannot meet its burden of showing coverage. (*Tribeca Broadway Assoc. v Mount Vernon Fire Ins. Co.*, 5 AD3d 198; *Munzer v St. Paul Fire & Mar. Ins. Co.*, 145 AD2d 193; *Bretton v Mutual of Omaha Ins. Co.*, 110 AD2d 46; *Caporino v Travelers Ins. Co.*, 62

NY2d 234; *Jones v St. Paul Fire & Mar. Ins. Co.*, 295 AD2d 569; *United States Fire Ins. Co. v General Reins. Corp.*, 949 F2d 569; *Loblaw, Inc. v Employers' Liab. Assur. Corp.*, 85 AD2d 880, 57 NY2d 872; *Standard Mar. Ins. Co. v Federal Ins. Co.*, 39 AD2d 444; *Eagle Leasing Corp. v Hartford Fire Ins. Co.*, 540 F2d 1257.) II. Three exclusions apply and act as a bar to coverage of Universal American Corp.'s claims. (*Citigroup Global Mkts. Inc. v Abbar*, 761 F3d 268; *Securities Inv. Protection Corp. v Morgan, Kennedy & Co., Inc.*, 533 F2d 1314; *Swerdloff v Miami Natl. Bank*, 584 F2d 54; *Arkwright Corp. v United States*, 53 F Supp 359; *Matter of Bombay Realty Corp. v Magna Carta*, 100 NY2d 124; *Muzak Corp. v Hotel Taft Corp.*, 1 NY2d 42; *Brooklyn City R.R. Co. v Kings County Trust Co.*, 214 App Div 506, 242 NY 531; *People v Bhatt*, 160 Misc 2d 973.) *Anderson Kill P.C.*, New York City (Joshua Gold and Dennis J. Nolan of counsel), and *Amy Bach*, *United Policyholders*, San Francisco, California, for *United Policyholders*, amicus curiae.

I. It is critically important that New York's courts provide policyholders with relief for improper denials of insurance coverage. (*American Home Prods. Corp. v Liberty Mut. Ins. Co.*, 565 F Supp 1485, 748 F2d 760; *Bi-Economy Mkt., Inc. v Harleysville Ins. Co. of N.Y.*, 10 NY3d 187.)

II. New York law, properly applied, requires a finding of insurance coverage for appellant's crime loss. (*Miller v Continental Ins. Co.*, 40 NY2d 675; *Seaboard Sur. Co. v Gillette Co.*, 64 NY2d 304; *Matter of Mostow v State Farm Ins. Cos.*, 88 NY2d 321; *Matter of Reliance Ins. Co.*, 55 AD3d 43, 12 NY3d 725; *Matter of New York Cent. Mut. Fire Ins. Co. v Ward*, 38 AD3d 898; *Retail Ventures, Inc. v National Union Fire Ins. Co. of Pittsburgh, Pa.*, 691 F3d 821.) III. Policyholders are particularly vulnerable when insurance companies are not compelled to honor their coverage obligations. (*Bi-Economy Mkt., Inc. v Harleysville Ins. Co. of N.Y.*, 10 NY3d 187.) IV. The lower courts' findings regarding insurance coverage intent were erroneous. (*Dean v Tower Ins. Co. of N.Y.*, 19 NY3d 704; *Cragg v Allstate Indem. Corp.*, 17 NY3d 118; *Rubin v Empire Mut. Ins. Co.*, 57 Misc 2d 104, 32 AD2d 1, 25 NY2d 426.)

## \*678 OPINION OF THE COURT

Rivera, J.

On this appeal we consider whether an insuring agreement for computer systems fraud that applies to “a fraudulent entry . . . of Electronic Data or Computer Program” encompasses losses caused by an authorized user's submission of fraudulent information into the insured's computer system. We conclude that the agreement is unambiguous and “fraudulent entry” refers **\*\*2** to unauthorized access into plaintiff's computer system, and not to content submitted by authorized users. Therefore, we affirm the order of the Appellate Division.

Plaintiff, Universal American Corp. (Universal), is a health insurance company that offers, as relevant to this appeal, a choice of federal government-regulated alternatives to Medicare, known as “Medicare Advantage Private Fee-For-Service” plans (Medicare Advantage).<sup>\*</sup> These plans allow Medicare-eligible individuals to purchase health insurance from private insurance companies, and those companies are, in turn, eventually reimbursed by the U.S. Department of Health & Human Services' Centers for Medicare & Medicaid Services for health care services provided to the plans' members. Universal has a computerized billing system that allows health care providers to submit claims directly to the system. According to Universal, the great majority of claims submitted are processed, approved, and paid automatically, without manual review.

The matter before us involves Universal's demand for indemnification to cover losses resulting from health care claims for unprovided services, paid through Universal's computer system. At issue is the coverage available to Universal pursuant to rider No. 3 (rider) of a financial institution bond (bond), issued by defendant National Union Fire Insurance Company of Pittsburgh, Pa. (National Union). The bond insured Universal against various losses, inclusive of certain losses resulting from dishonest and fraudulent acts. The rider amended the bond to provide indemnification specifically for computer systems fraud, and states, in part:

“COMPUTER SYSTEMS

“It is agreed that:

**\*679** “1. the attached bond is amended by adding an Insuring Agreement as follows:

“COMPUTER SYSTEMS FRAUD

“Loss resulting directly from a fraudulent

“(1) entry of Electronic Data or Computer Program into, or

**\*\*3** “(2) change of Electronic Data or Computer Program within

“the Insured's proprietary Computer System . . .

“provided that the entry or change causes

“(a) Property to be transferred, paid or delivered,

“(b) an account of the insured, or of its customer, to be added, deleted, debited or credited, or

“(c) an unauthorized account or a fictitious account to be debited or credited.”

The rider, and the basic bond coverage, carry a \$10 million limit and a \$250,000 deductible for each “single loss,” which, as defined in the rider, includes “the fraudulent acts of one individual,” or of “unidentified individuals but arising from the same method of operation.” Universal's annual premium during the relevant policy period was \$170,500.

A few months after obtaining coverage, Universal suffered over \$18 million in losses for payment of fraudulent claims for services never actually performed under its Medicare Advantage plans. When Universal sought payment from National Union for its post-deductible losses, National Union denied coverage on the ground that the rider did not encompass losses for Medicare fraud, which National Union described as losses from payment for claims submitted by health care providers.

Universal then commenced an action for damages and declaratory relief against National Union. Thereafter, Universal moved pursuant to [CPLR 3212](#) for partial summary judgment, and an order declaring the losses to be covered under the

policy. National Union cross-moved for summary judgment. Supreme Court denied Universal's motion, granted National Union's motion, and dismissed the complaint (38 Misc 3d 859 [Sup Ct, NY County 2013]), concluding that the rider is not ambiguous and does not extend to fraudulent claims entered into Universal's system by authorized users. The court \*680 determined, instead, that the intended coverage is for an unauthorized entry into the computer system by a hacker or through a computer virus.

The Appellate Division unanimously modified the summary judgment order, on the law, to declare the policy does not cover the loss, and otherwise affirmed. The Court concluded the unambiguous language of the policy does not cover fraudulent content entered by authorized users, but rather “wrongful acts in manipulation of the computer system, i.e., by hackers” (110 AD3d 434, 434 [1st Dept 2013]). We granted Universal leave to appeal (23 NY3d 904 [2014]), and now affirm.

An insurance agreement is subject to principles of contract interpretation. “As with the construction of contracts generally, ‘unambiguous provisions of an insurance contract \*\*4 must be given their plain and ordinary meaning, and the interpretation of such provisions is a question of law for the court’ ” (*Vigilant Ins. Co. v Bear Stearns Cos., Inc.*, 10 NY3d 170, 177 [2008], quoting *White v Continental Cas. Co.*, 9 NY3d 264, 267 [2007]). “Ambiguity in a contract arises when the contract, read as a whole, fails to disclose its purpose and the parties' intent” (*Ellington v EMI Music, Inc.*, 24 NY3d 239, 244 [2014], citing *Brooke Group v JCH Syndicate 488*, 87 NY2d 530, 534 [1996]), or where its terms are subject to more than one reasonable interpretation (see *Dean v Tower Ins. Co. of N.Y.*, 19 NY3d 704, 708 [2012], quoting *Seaboard Sur. Co. v Gillette Co.*, 64 NY2d 304, 311 [1984]; *Chimart Assoc. v Paul*, 66 NY2d 570, 573 [1986] [ambiguity exists if “the agreement on its face is reasonably susceptible of more than one interpretation”]; see also *Greenfield v Philles Records*, 98 NY2d 562, 569-570 [2002]). However, parties cannot create ambiguity from whole cloth where none exists, because provisions “are not ambiguous merely because the parties

interpret them differently” (*Mount Vernon Fire Ins. Co. v Creative Hous.*, 88 NY2d 347, 352 [1996]). Rather, “the test to determine whether an insurance contract is ambiguous focuses on the reasonable expectations of the average insured upon reading the policy and employing common speech” (*Matter of Mostow v State Farm Ins. Cos.*, 88 NY2d 321, 326-327 [1996] [citations omitted]; see also *Cragg v Allstate Indem. Corp.*, 17 NY3d 118, 122 [2011] [“Insurance contracts must be interpreted according to common speech and consistent with the reasonable expectations of the average insured”]).

Turning to the language of the rider, we conclude that it unambiguously applies to losses incurred from unauthorized access \*681 to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users. The term “fraudulent” is not defined in the rider, but it refers to deceit and dishonesty (see Merriam-Webster Collegiate Dictionary 464 [10th ed 1993]). While the rider also does not define the terms “entry” and “change,” the common definition of the former includes “the act of entering” or “the right or privilege of entering,” “access,” and the latter means “to make different,” “alter” (*id.* at 387, 190). In the rider, “fraudulent” modifies “entry” or “change” of electronic data or computer program, meaning it qualifies the act of entering or changing data or a computer program. Thus, the rider covers losses resulting from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be “hacking” of the computer system. The rider's reference to “fraudulent” does not also qualify what is actually acted upon, namely the “electronic data” or “computer program” itself. The intentional word placement of “fraudulent” before “entry” and “change” manifests the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access.

Other language in the rider confirms that the rider seeks to address unauthorized access. First, the rider is captioned “COMPUTER SYSTEMS,” and the specific language at issue is found under the subtitle “COMPUTER SYSTEMS FRAUD.”



These headings clarify that the rider's **\*\*5** focus is on the computer system qua computer system. Second, under "EXCLUSIONS," the rider exempts from coverage losses resulting directly or indirectly from fraudulent instruments "which are used as source documentation in the preparation of Electronic Data or manually keyed into a data terminal." If the parties intended to cover fraudulent content, such as the billing fraud involved here, then there would be no reason to exclude fraudulent content contained in documents used to prepare electronic data, or manually keyed into a data terminal.

Nonetheless, Universal argues that in the context of the rider, "fraudulent entry" means "fraudulent input" because a loss due to a fraudulent entry by necessity can only result from the input of fraudulent information. This would render superfluous the word "a" before "fraudulent," and the word "of" before "electronic data or computer program." Universal's proposed interpretation is easily achieved by providing coverage for a "loss resulting directly from fraudulent data." Of **\*682** course, that is not what the rider says. Moreover, Universal's reading ignores the other language contained in the rider and its categorical application to "Computer Systems" and "Computer Systems Fraud."

We are also unpersuaded by Universal's reliance on *Owens, Schine & Nicola, P.C. v Travelers Cas. & Sur. Co. of Am.* (2010 WL 4226958, \*1, 2010 Conn Super LEXIS 2386, \*1-3 [Sept. 20, 2010, No. CV095024601], vacated 2012 WL 12246940, 2012 Conn Super LEXIS 5053 [Apr. 18, 2012] [memorandum of decision vacated by stipulation of the parties]), in support of its argument that the heading "COMPUTER SYSTEMS FRAUD" can reasonably be interpreted to encompass fraud committed through a computer, meaning fraud that is not limited to computer hacking incidents. The *Owens* decision is of little assistance to Universal's cause. In *Owens*, the policy provision was far broader, and contained an internally applicable definition of "Computer Fraud" as

"[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises:

"1. to a person (other than a Messenger) outside the Premises or Banking Premises; or

"2. to a place outside the Premises or Banking Premises" (2010 WL 4226958, \*4, 2010 Conn Super LEXIS 2386, \*9-10).

The insurer argued that "computer fraud" within the meaning of the policy required manipulation of the computer system, i.e., hacking. It further argued that there was no actual computer fraud because the use of emails and a computer to create a fraudulent check, as part of a scheme to steal funds from the insured, did not cause the physical transfer of money out of the insured's account. Instead, the loss resulted from the insured's wiring of the funds out of the account. The court found the phrase "use of any computer" to be ambiguous as to "the amount of computer usage necessary to constitute computer fraud" (2010 WL 4226958, \*7, 2010 Conn Super LEXIS 2386, \*19). Thus, *Owens* was concerned with whether the computer had been utilized sufficiently to constitute computer fraud as contemplated by the parties, based on their reasonable understanding of the policy's terms.

Here, it is undisputed that use of Universal's computer is absolutely essential to trigger coverage for a loss, and that its **\*683** computers were indeed used in a manner that resulted in payment of claims for health care services that were never provided. Thus, unlike in *Owens*, the **\*\*6** question is not how much computer use is required under the policy, but whether the use involved here is the type actually covered by the rider.

We conclude that the "reasonable expectations of the average insured upon reading the policy" (*Mostow*, 88 NY2d at 326-327) are that the rider applies to losses resulting directly from fraudulent access, not to losses from the content submitted by authorized users. Accordingly, the order of the Appellate Division should be affirmed, with costs.

Judges Read, Pigott, Abdus-Salaam, Stein and Fahey concur; Chief Judge Lippman taking no part.

Order affirmed, with costs.

Copr. (C) 2018, Secretary of State, State of New York

## FOOTNOTES

### Footnotes

- \* Medicare, a hospital, medical, and prescription drug insurance program, is administered by the Centers for Medicare & Medicaid Services within the U.S. Department of Health & Human Services (see [42 USC § 1395 et seq.](#)).

---

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.



## Apache Corporation v. Great American Insurance Company

United States Court of Appeals, Fifth Circuit. | October 18, 2016 | 662 Fed.Appx. 252 | 2016 WL 6090901


### Document Details

standard Citation: Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016)  
All Citations: 662 Fed.Appx. 252

### Search Details

Jurisdiction: Texas

### Delivery Details

Date: May 9, 2018 at 4:24 PM  
Delivered By: Juan Luis Garcia  
Client ID: 099998/099580 PRACTICE DEVELOPMENT  
Status Icons: 

### Outline

[Synopsis](#) (p.1)  
[Attorneys and Law Firms](#) (p.1)  
[Opinion](#) (p.1)  
[All Citations](#) (p.7)

662 Fed.Appx. 252

This case was not selected for publication in West's Federal Reporter.

See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also U.S.Ct. of App. 5th Cir. Rules 28.7 and 47.5. United States Court of Appeals, Fifth Circuit.

APACHE CORPORATION,  
Plaintiff–Appellee Cross–Appellant  
v.  
GREAT AMERICAN INSURANCE  
COMPANY, Defendant–  
Appellant Cross–Appellee

No. 15–20499

|  
Date Filed: 10/18/2016

#### Synopsis

**Background:** Insured filed state court suit against insurer, challenging denial of claim under crime-protection insurance policy, for approximately \$2.4 million loss sustained from criminals defrauding insured, partly by using e-mail from incorrect website address for vendor instructing insured to use new bank account for making payments to vendor, which insured followed after flawed follow-up investigation and made authorized payments for vendor's legitimate invoices to criminals' fraudulent bank account. Following removal, the United States District Court for the Southern District of Texas, [Alfred H. Bennett, J.](#), [2015 WL 7709584](#), granted insured summary judgment. Insurer appealed.

**[Holding:]** The Court of Appeals held that loss was not covered under policy's computer fraud provision.

Vacated and judgment rendered for insurer.

Appeals from the United States District Court for the Southern District of Texas, USDC No. 4:14–CV–237

#### Attorneys and Law Firms

[Patrick W. Mizell](#), [Deborah Carleton Milner](#), [Vinson & Elkins, L.L.P.](#), [David H. Brown](#), Attorney, [Brown & Kornegay, L.L.P.](#), Houston, TX, for Plaintiff–Appellee Cross–Appellant.

[Francis Joseph Nealon](#), [Michael Albert Graziano](#), Attorney, [Eckert, Seamans, Cherin & Mellott, L.L.C.](#), Washington, DC, [William Gaynor Winget](#), \*253 [Harris Bruce Katz](#), [Garry T. Stevens, Jr.](#), New York, NY, [Martin Samuel Schexnayder](#), Esq., Houston, TX, [Winget, Spadafora & Schwartzberg, L.L.P.](#), for Defendant–Appellant Cross–Appellee.

[Michael Keeley](#), [Carla Cash Crapster](#), [Strasburger & Price, L.L.P.](#), Dallas, TX, for Amicus Curiae Surety & Fidelity Association of America.

Before [JOLLY](#), [BARKSDALE](#), and [SOUTHWICK](#), Circuit Judges.

#### Opinion

PER CURIAM \*

Texas law controls this diversity action, which arises out of Apache Corporation's being defrauded by criminals, in part by their use of an email; as a result of the fraud, and a flawed follow-up investigation by Apache, it made authorized payments of legitimate invoices from its vendor to the criminals' bank account, instead of to its vendor's. Great American Insurance Company (GAIC), Apache's insurer, denied its claim for coverage of its loss under GAIC's “Computer Fraud” provision of Apache's crime-protection insurance policy. At issue is whether the district court correctly awarded summary judgment to Apache, on the basis that its loss was covered under that provision; and, if so, whether the court properly denied statutory penalties, subject to [Texas Insurance Code § 542.060](#). VACATED and RENDERED.



I.

GAIC is headquartered in Ohio; Apache is an oil-production company, with its principal place of business in Houston, Texas, but operating internationally. In March 2013, during the coverage period for Apache's policy with GAIC, an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed Apache to change the bank-account information for its payments to Petrofac. The Apache employee replied that the change-request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts-payable department received an email from a "petrofacld.com" address. But, Petrofac's authentic email domain name is "petrofac.com"; the criminals created "petrofacld.com" to send the fraudulent email. The email advised: Petrofac's "accounts details have now been changed"; and "[t]he new account takes ... immediate effect and all future payments must now be made into this account". As noted in the email, an attachment to it was a signed letter on Petrofac letterhead, providing both old-bank-account information and the new-bank-account number, with instructions to "use the new account with immediate effect". In addition, the email stated: the "attached letter ... has also been posted to you".

In response, an Apache employee called the telephone number provided on the letterhead to verify the request and concluded the call confirmed the authenticity of the change-request; next, a different Apache employee approved and implemented the change. A week later, Apache was transferring funds for payment of Petrofac's invoices to the new bank account.

Within one month, however, Apache received notification Petrofac had not received the £4.3 million (approximately \$7 million) Apache had transferred to the new (fraudulent) account. After an investigation \*254 determined the criminals were likely based in Latvia, Apache recouped

a substantial portion of the funds. It contends, however, it suffered a loss, before the \$1 million policy deductible, of approximately £1.5 million (approximately \$2.4 million).

Apache submitted a claim to GAIC, asserting coverage under the "Computer Fraud" provision, which states:

We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:

- a. to a person (other than a messenger) outside those premises; or
- b. to a place outside those premises.

In its denial letter, GAIC advised Apache's "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds".

Apache initiated this action in Texas state court in January 2014 against GAIC for denying its claim under the computer-fraud provision. After GAIC removed the action to district court, both parties moved for summary judgment.

The court denied GAIC's motion and granted Apache's, ruling, *inter alia*, "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor' ". [Apache Corp. v. Great Am. Ins. Co., Civil Action No. 4:14-CV-237, 2015 WL 7709584, at \\*3 \(S.D. Tex. 7 Aug. 2015\)](#). Moreover, the court reasoned that, if the policy only covered losses due to computer hacking, such an interpretation would render the policy "pointless". *Id.*

Apache moved for entry of final judgment, and sought, *inter alia*, statutory penalties under [Texas Insurance Code § 542.060](#). But, in entering judgment, the court denied the penalties.

## II.

GAIC challenges the summary judgment awarded Apache; on the other hand, Apache challenges the denial of statutory penalties. Because we vacate the judgment and render it for GAIC, we do not reach the penalties issue.

A summary judgment is reviewed *de novo*. *E.g.*, [Southern Ins. Co. v. Affiliated FM Ins. Co.](#), 830 F.3d 337, 343 (5th Cir. 2016). Summary judgment is proper if the movant shows no genuine dispute as to any material fact and entitlement to judgment as a matter of law. *Fed. R. Civ. P.* 56(a). “The court must view the facts developed below in the light most favorable to the nonmoving party.” *La. Generating, L.L.C. v. Ill. Union Ins. Co.*, 831 F.3d 618, 622 (5th Cir. 2016). A genuine dispute of material fact exists “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party”. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). Interpretation of an insurance policy presents a question of law; therefore it is also reviewed *de novo*. *E.g.*, *Naquin v. Elevating Boats, L.L.C.*, 817 F.3d 235, 238 (5th Cir. 2016).

The summary-judgment record is very limited—there were no depositions or discovery responses. For its motion, GAIC attached: Apache's proof of loss and supporting documents, such as the email at issue and the letterhead attachment to it; the crime-protection policy; and Apache's declination letter. Apache relied on GAIC's exhibits, in addition to two very brief, self-serving declarations executed by two Apache employees.

As noted, Texas law controls this diversity action. GAIC claims, *inter alia*, the loss was not a covered occurrence because: \*255 the email did not “cause a transfer”; and coverage under this provision is “unambiguously limited” to losses from “hacking and other incidents of unauthorized computer use”. GAIC notes that, under Texas law, insurance provisions are interpreted according to the same rules applicable to contracts generally; but, it also asserts the “Supreme Court of Texas has ‘repeatedly stressed the importance of uniformity

when identical insurance provisions will necessarily be interpreted in various jurisdictions’ ”, citing [McGinnes Indus. Maint. Corp. v. Phoenix Ins. Co.](#), 477 S.W.3d 786, 794 (Tex. 2015). According to GAIC, the weight of authorities interpreting similar computer-fraud language, considered with Texas' policy goal of cross-jurisdictional uniformity, persuades against coverage for Apache's claim.

Apache counters that the plain meaning of the computer-fraud language covers its loss, and maintains any ambiguity in the terms should be resolved in favor of the insured's reasonable interpretation, even if the insurer's interpretation is more reasonable, relying on [RSUI Indem. Co. v. Lynd Co.](#), 466 S.W.3d 113, 118 (Tex. 2015). Because the language of the provision says nothing about “hacking”, Apache asserts it only needs to show that “any computer was used to fraudulently cause the transfer of funds”.

As noted, under Texas law, courts interpret insurance policies using the same rules of construction applicable to contracts generally. [Tesoro Ref. & Mktg. Co., L.L.C. v. Nat'l Union Fire Ins. Co. of Pitt., Pa.](#), 833 F.3d 470, 474 (5th Cir. 2016); [Am. Mfrs. Mut. Ins. Co. v. Schaefer](#), 124 S.W.3d 154, 157 (Tex. 2003). The policy must be construed such that no provision is rendered meaningless. [Tesoro](#), 833 F.3d at 474 (citing [Schaefer](#), 124 S.W.3d at 157).

Mere disagreement about the meaning of a contract does not render it ambiguous. *Id.* “A contract is ambiguous only when the application of pertinent rules of interpretation to the face of the instrument leaves it genuinely uncertain which one of two or more meanings is the proper meaning.” *Id.* (quoting [RSUI Indem.](#), 466 S.W.3d at 119). The ambiguity, *vel non*, of an insurance provision is a question of law; if ambiguity is found, the court must adopt the interpretation favoring the insured. *Id.* (citing [RSUI Indem.](#), 466 S.W.3d at 118; [Schaefer](#), 124 S.W.3d at 157).

As also noted, the Texas Supreme Court has stressed its policy preference for “uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions”. [McGinnes](#), 477

[S.W.3d at 794](#) (responding to fifth circuit certified question). And, even when uniformity is made impossible by jurisdictional splits, Texas courts “strive for uniformity as much as possible”. *Id.* (internal quotation marks omitted) (quoting *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 824 (Tex. 1997)).

For our *Erie*-guess, the parties agree that only the computer-fraud provision is at issue. In contending Apache's loss is not covered under it because the loss did not, as required by the provision, “result[ ] directly from the use of any computer to fraudulently cause a transfer”, GAIC maintains the transfer of funds to the fraudulent bank account resulted from other events: before the email, the telephone call directing Apache to change the account information; and, after the email, the telephone call by Apache to the criminals to confirm the change-request, followed by the Apache supervisor's review and approval of the emailed request, Petrofac's submission of invoices, the review and approval of them by Apache employees, and Apache's authorized and intentional transfer of funds, even though to the fraudulent bank account. (As discussed, the email \*256 stated that the attached letter on Petrofac letterhead “has also been posted [mailed] to” Apache. There is no evidence in the summary-judgment record, however, that Apache received a hardcopy of the letter. Nor is there any evidence Apache relied on one, as opposed to the electronic version attached to the fraudulent email, in telephoning to confirm the information provided. In any event, although this mailed-letter point was presented by GAIC at oral argument here, it is waived because it was not raised in district court or in GAIC's opening brief on appeal, with the alleged mailing of the letter only noted belatedly in its reply brief.)

In response to GAIC's position, Apache claims the loss is covered, based on the “commonly understood meaning” of the computer-fraud-provision's terms. It asserts GAIC attempts to add terms it wishes had been included in the provision.

The parties do not cite any Texas authority interpreting “the use of any computer to

fraudulently cause a transfer” in the context of the computer-fraud provision, nor have we found any. Instead, GAIC relies primarily on unpublished opinions as persuasive authority; none are by Texas courts and almost all are outside our circuit. Apache attempts to distinguish them. Bearing in mind the limited weight accorded such non-binding authority, as well as Texas' policy preference for cross-jurisdictional uniformity, a detailed—albeit numbing—analysis of the cited authorities is required. *See McGinnes*, 477 S.W.3d at 794.

GAIC cites the ninth circuit's decision in *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, affirming coverage-denial under a similarly worded computer-fraud provision. (*Pestmaster II*), No. 14–56294, 656 Fed.Appx. 332, 333, 2016 WL 4056068, at \*1 (9th Cir. 29 July 2016), *aff'g* *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.* (*Pestmaster I*), No. CV 13–5039–JFW, 2014 WL 3844627 (C.D. Cal. 17 July 2014) (unpublished). That policy defined “computer fraud” as “[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property”. *Pestmaster I*, 2014 WL 3844627, at \*4.

The underlying fraud was committed by a payroll contractor against the insured. *Id.* at \*1. The contractor had been hired, *inter alia*, to withhold and submit payments for the insured's payroll taxes. *Id.* To that end, the contractor prepared invoices for the insured, and was authorized to initiate transfers of funds from the insured to the contractor's bank account, in order to pay invoices approved by the insured. *Id.* (The district court considered the contractor's initiating the transfer of funds as the relevant “use of a computer”. *Id.* at \*7–8.) Instead of paying the approved invoices, the contractor fraudulently used the insured's funds to pay her own expenses, ultimately leaving the insured indebted to the Internal Revenue Service for payroll taxes. *Id.* at \*2, 7–8.

The insured filed an action after being denied coverage under the crime-protection policy for the tax debt; but, the district court rejected coverage under the computer-fraud provision because the “claimed losses did not ‘flow immediately’ and ‘directly’ from [the contractor's] use of a computer”.

*Id.* at \*8. “[T]here was no loss when funds were initially transferred to [the contractor] because the transfers were authorized by [the insured]”. *Id.*

In affirming, the ninth circuit interpreted “the phrase ‘fraudulently cause a transfer’ to require an unauthorized transfer of funds”. *Pestmaster II*, 2016 WL 4056068, at \*1. “Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some \*257 point in the transaction would convert this Crime Policy into a ‘General Fraud’ Policy”, essentially covering losses from all forms of fraud rather than a specified risk category. *Id.*

GAIC also cites *Brightpoint, Inc. v. Zurich Am. Ins. Co.*, in which a district court ruled similar policy language did not cover a loss claimed by an insured distributor of prepaid mobile-telephone cards. No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, at \*7 (S.D. Ind. 10 March 2006) (unpublished). After the distributor received a facsimile-transmission of purchase orders, postdated checks, and bank guarantees from a purported customer, the distributor delivered the inventory in exchange for the original documents. *Id.* at \*2. The transaction was a fraud, with the distributor's never receiving payment. *Id.* at \*3.

The court assumed, without deciding, that the facsimile-transmission constituted “use of a computer”. In concluding the loss was not covered, it stated:

We do not view the faxed [documents] to have “fraudulently cause[d] a transfer” of the phone cards, as required under the policy definition of “Computer Fraud.” ... [T]he facsimile simply alerted the [insured] to the fact that [the insured's customer], or perhaps in this case some other person mimicking his methods, wished to place an order. Only after [the insured] received the physical

documents would [it] release the phone cards and, based on established practices of [the insured], the cards would not have been turned over simply on the basis of the facsimile.

*Id.* at \*7.

Additionally, GAIC points to a summary-judgment ruling in its favor by the Northern District of Texas. See *GAIC v. AFS/IBEX Fin. Servs., Inc.*, No. 3:07-CV-924-O, 2008 WL 2795205, at \*2 (N.D. Tex. 21 July 2008) (unpublished). There, an employee of the insured insurance-premium-finance company used a computer to submit more than 100 false loan applications to induce the insured to issue checks that the employee deposited for personal use. *Id.* The insured's claim with GAIC sought coverage under, *inter alia*, the computer-fraud provision of a crime-protection insurance policy; the claim was denied. *Id.*

As in this instance, the computer-fraud provision covered a loss “resulting directly from the use of any computer to fraudulently cause a transfer of ... property”. *Id.* at \*14. The court interpreted this language as being “designed to cover losses *directly* stemming from fraud perpetrated by use of a computer”. *Id.* (emphasis in original). Notably, the insured did not present “any evidence or arguments in opposition” to GAIC's claiming the provision did not apply, but the court nonetheless determined the loss was not covered. *Id.*

As GAIC notes, similar policy language was at issue in *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, but the court denied the insurer's motion to dismiss and allowed the insured's claim to go forward. No. 11-6187, 2012 WL 1067694, at \*4 (D. N.J. 29 March 2012) (unpublished). The facts considered in *Vonage*, however, differ from those here, because the insured was unquestionably “hacked”—hackers gained access to the insured's servers to fraudulently route international telephone calls. *Id.* at \*1.

The only decision discussed by the parties which ruled the policy language covered computer-use limited to email communications was later vacated by the Superior Court of Connecticut. See *Owens*,

*Schine, & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, 50 Conn. L. Rptr. 665, 2010 WL 4226958, at \*8 (Conn. Super. Ct. 20 Sept. 2010) (unpublished), \*258 vacated, 2012 WL 12246940 (Conn. Super. Ct. 18 Apr. 2012) (unpublished). The policy at issue defined “computer fraud” as “[t]he use of any computer to fraudulently cause a transfer”. *Id.* at \*4.

The insured, a law firm, was defrauded by criminals who sent emails to the firm, representing themselves as Chinese businessmen in need of legal services. *Id.* at \*1. All communications between the firm and the criminals were carried out by email. *Id.* at \*7. A retainer agreement was signed, scanned, and emailed to the firm by the criminals. *Id.* at \*1. They claimed they needed the firm's services to collect a debt owed by an American company. *Id.* After a fraudulent check was received by the firm from the supposed debtor, the firm deposited the check in its trust account. *Id.* The firm then successfully wired funds from that account to one in South Korea; but, after the firm's bank discovered the fraud, it refused to honor the fraudulent check provided by the criminals to the firm, resulting in its financial loss. *Id.* at \*2.

In denying the insurer's summary-judgment motion, the court ruled “[t]he emails were the proximate cause and ‘efficient cause’ of [the insured's] loss because the [emails] set the chain of events in motion that led to the entire loss”. *Id.* at \*8. As discussed, the decision, however, was vacated by the very court that rendered it.

Again, this vacated trial-court ruling is the only presented decision interpreting the computer-fraud policy language to cover a loss when the computer use at issue was limited to email correspondence. Therefore, with the exception of the district court's ruling at issue, there is cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use.

Here, the “computer use” was an email with instructions to change a vendor's payment information and make “all future payments” to it; the email, with the letter on Petrofac

letterhead as an attachment, followed the initial telephone call from the criminals and was sent in response to Apache's directive to send the request on the vendor's letterhead. Once the email was received, an Apache employee called the telephone number provided on the fraudulent letterhead in the attachment to the email, instead of, for example, calling an independently-provided telephone contact for the vendor, such as the pre-existing contact information Apache would have used in past communications. Doubtless, had the confirmation call been properly directed, or had Apache performed a more thorough investigation, it would never have changed the vendor-payment account information. Moreover, Apache changed the account information, and the transfers of money to the fraudulent account were initiated by Apache to pay legitimate invoices.

The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*, convert the computer-fraud provision to one for general fraud. See 2016 WL 4056068, at \*1. We take judicial notice that, when the policy was issued in 2012, electronic communications were, as they are now, ubiquitous, and even the line between “computer” and “telephone” was already blurred. In short, few—if any—fraudulent schemes would not involve some form of computer-facilitated communication.

This is reflected in the evidence at hand. Arguably, Apache invited the computer-use at issue, through which it now seeks \*259 shelter under its policy, even though the computer-use was but one step in Apache's multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent bank account.

The email was sent only after Apache's advising, in reply to the criminals' change-request telephone call, that the request had to be made on Petrofac letterhead. The criminals complied: by attaching to the email (sent using a slightly different domain



name) a letter on altered letterhead; and, as stated in the email, by allegedly mailing that letter to Apache. Accordingly, the computer-use was in response to Apache's refusing, during the telephone call, to, for example, transcribe the change-request, which it could have then investigated with its records.

No doubt, the better, safer procedure was to require the change-request to be made on letterhead, especially for future payment of Petrofac's very large invoices. But the request must still be investigated properly to verify it is legitimate. In any event, based on the evidence in the summary-judgment record, Apache followed-up on the request in the email and its attachment. In other words, the authorized transfer was made to the fraudulent account only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it.

Moreover, viewing the multi-step process in its simplest form, the transfers were made not because of fraudulent information, but because Apache

elected to pay legitimate invoices. Regrettably, it sent the payments to the wrong bank account. Restated, the invoices, not the email, were the reason for the funds transfers.

In sum, and applying Texas law in making this *Erie* guess, both the plain meaning of the policy language, as well as the uniform interpretations across jurisdictions, dictate Apache's loss was not a covered occurrence under the computer-fraud provision. See *McGinnes*, 477 S.W.3d at 794.

### III.

For the foregoing reasons, the judgment is VACATED and judgment is RENDERED for Great American Insurance Company.

### All Citations

662 Fed.Appx. 252

### Footnotes

- \* Pursuant to 5th Cir. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5th Cir. R. 47.5.4.

681 Fed.Appx. 627

This case was not selected for publication in West's Federal Reporter. See Fed. Rule of Appellate Procedure 32.1 generally governing citation of judicial decisions issued on or after Jan. 1, 2007. See also U.S.Ct. of App. 9th Cir. Rule 36-3. United States Court of Appeals, Ninth Circuit.

**TAYLOR & LIEBERMAN**, an Accountancy Corporation, Plaintiff-Appellant,  
v.  
FEDERAL INSURANCE COMPANY,  
a corporation, Defendant-Appellee.

No. 15-56102

Argued and Submitted February  
13, 2017 Pasadena, California

Filed March 9, 2017

**Synopsis**

**Background:** Insured accounting firm brought action against insurer for breach of insurance coverage contract based on insurer's denial of coverage for insured's loss of client's funds as result of transfers that insured made in response to e-mails from perpetrator who had fraudulently taken over client's e-mail account. The United States District Court for the Central District of California, [Ronald S.W. Lew, J.](#), 2015 WL 3824130, granted summary judgment to insurer. Insured appealed.

**Holdings:** The Court of Appeals held that:

- [1] policy's coverage for forgery did not apply;
- [2] policy's coverage for computer fraud did not apply; and
- [3] policy's coverage for funds transfer fraud did not apply.

Affirmed.

Appeal from the United States District Court for the Central District of California, \*628 Ronald S.W. Lew, District Judge, Presiding, D.C. No. 2:14-cv-03608-RSWL-SH

**Attorneys and Law Firms**

[Robert Douglas Whitney](#), Edison, McDowell & Hetherington LLP, Oakland, CA, [Jeffrey N. Williams](#), [Raymond J. Tittmann](#), Wargo & French LLP, Los Angeles, CA, for Plaintiff-Appellant

[Gary John Valeriano](#), [Kenneth Watnick](#), Attorney, Anderson, McPharlin & Connors LLP, Los Angeles, CA, for Defendant-Appellee

Before: [M. SMITH](#) and [OWENS](#), Circuit Judges,  
and [KORMAN](#), \* District Judge.

**MEMORANDUM\*\***

Taylor & Lieberman ("T&L") appeals from the district court's order granting Federal Insurance Company's ("FIC") motion for summary judgment. As the parties are familiar with the facts, we do not recount them here. We have jurisdiction under 28 U.S.C. § 1291, and we affirm on other grounds.<sup>1</sup>

[1] **1. There is no forgery coverage.** The policy provides coverage for an insured's direct loss "resulting from Forgery or alteration of a Financial Instrument by a Third Party." Relying on the "Last Antecedent Rule,"<sup>2</sup> T&L argues that the words "financial instrument" only limit coverage for an alteration, and that a covered forgery need not be of a financial instrument.

Not so. An exception to the last antecedent rule "provides that when several words are followed by a clause that applies as much to the first and other words as to the last, the natural construction of the language demands that the clause be read as applicable to all." *People ex rel. Lockyer v. R.J. Reynolds Tobacco Co.*, 107 Cal.App.4th 516, 132 Cal.Rptr.2d 151, 162 (2003) (internal quotation marks omitted). Moreover, where, as here, a clause

only has two antecedents, the force of the last antecedent rule “diminishes ... in accordance with ordinary English usage.” *Old Republic Constr. Program Grp. v. Boccardo Law Firm, Inc.*, 230 Cal.App.4th 859, 179 Cal.Rptr.3d 129, 139 n.6 (2014). Accordingly, under a natural reading of the policy, forgery coverage only extends over the forgery of a financial instrument.

Here, the emails instructing T&L to wire money were not financial instruments, like checks, drafts, or the like.<sup>3</sup> See *Vons Cos., Inc. v. Fed. Ins. Co.*, 57 F.Supp.2d 933, 945 (C.D. Cal. 1998) (holding that wire instructions, invoices, and purchase orders were not “documents of the same type and effect as checks and drafts.”). And even if the emails were considered equivalent to checks or drafts, they were not “made, drawn by, or drawn upon” T&L, the insured. Rather, they simply \*629 directed T&L to wire money from T&L's client's account. In sum, there is no forgery coverage.

**[2] 2. There is no computer fraud coverage.**

T&L also argues that the computer fraud coverage applies because the emails constituted an unauthorized (1) “entry into” its computer system, and (2) “introduction of instructions” that “propagate[d] themselves” through its computer system. These arguments are not well-taken.

First, there is no support for T&L's contention that sending an email, without more, constitutes an unauthorized entry into the recipient's computer system. See, e.g., *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1 Cal.Rptr.3d 32, 71 P.3d 296, 304 (2003) (holding that the “mere sending” of emails does not amount to actionable trespass to a computer system in the absence of “some actual or threatened interference with the computers' functioning”); see also *Spam Arrest, LLC v. Replacements, Ltd.*, No. C12-481RAJ, 2013 WL 4675919, at \*20 (W.D. Wash. Aug. 29, 2013) (“[N]o Ninth Circuit court has ever held that the mere act of sending an email constitutes access to a computer through which the email passes on the way to its recipient.”).

Second, the emails were not an unauthorized introduction of instructions that propagated themselves through T&L's computer system. The

emails instructed T&L to effectuate certain wire transfers. However, under a common sense reading of the policy, these are not the type of instructions that the policy was designed to cover, like the introduction of malicious computer code. See *Emp'rs Reinsurance Co. v. Superior Court*, 161 Cal.App.4th 906, 74 Cal.Rptr.3d 733, 744 (2008) (“We interpret words in accordance with their ordinary and popular sense, unless the words are used in a technical sense or a special meaning is given to them by usage.”). Additionally, the instructions did not, as in the case of a virus, propagate themselves throughout T&L's computer system; rather, they were simply part of the text of three emails.

Accordingly, under the plain meaning of the policy, the computer fraud coverage does not apply.

**[3] 3. There is no funds transfer fraud coverage.** Lastly, T&L is not entitled to funds transfer fraud coverage. Fraud transfer fraud encompasses:

fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver **Money or Securities** from any account maintained by an **Insured Organization** at such Institution, without an **Insured Organization's** knowledge or consent.

This coverage is inapplicable because T&L requested and knew about the wire transfers. After receiving the fraudulent emails, T&L directed its client's bank to wire the funds. T&L then sent emails confirming the transfers to its client's email address. Although T&L did not know that the emailed instructions were fraudulent, it did know about the wire transfers.

Moreover, T&L's receipt of the emails from its client's account does not trigger coverage because T&L is not a financial institution.<sup>4</sup> See *First Am. Title Ins. Co. v. XWarehouse Lending Corp.*, 177 Cal.App.4th 106, 98 Cal.Rptr.3d 801, 808 (2009)



\*630 (“[C]ourts will not indulge in a forced construction” where “the terms of a policy are plain.”).

**AFFIRMED.**

**All Citations**

In sum, there is no funds transfer coverage.

681 Fed.Appx. 627

**Footnotes**

- \* The Honorable Edward R. Korman, United States District Judge for the Eastern District of New York, sitting by designation.
- \*\* This disposition is not appropriate for publication and is not precedent except as provided by [Ninth Circuit Rule 36-3](#).
- 1 “[A] district court’s grant of summary judgment may be affirmed if it is supported by any ground in the record, whether or not the district court relied upon that ground.” [United States ex rel. Kelly v. Serco, Inc.](#), 846 F.3d 325, 330 (9th Cir. 2017).
- 2 Under this rule of construction, “qualifying words, phrases and clauses are to be applied to the words or phrases immediately preceding and are not to be construed as extending to or including others more remote.” [White v. Cnty. of Sacramento](#), 31 Cal.3d 676, 183 Cal.Rptr. 520, 646 P.2d 191, 193 (1982).
- 3 Under the policy, financial instruments include “checks, drafts or similar written promises, orders or directions to pay a sum certain in money, that are made, drawn by or drawn upon” an insured, its agent, “or that are purported to have been so made or drawn.”
- 4 Further, contrary to T&L’s argument, the policy provides no indication that the parties intended to adopt [31 U.S.C. § 5312\(a\)\(2\)](#)’s broad definition of a “financial institution,” which includes—among other things—pawnbrokers, travel agencies, and dealers in precious stones.

---

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.

(S.D.N.Y. June 15, 2017) (citing Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC, 797 F.3d 160, 191 (2d Cir. 2015)). An amended complaint must be filed no later than twenty-one days after the date of this opinion.

### Conclusion

For the foregoing reasons, Defendants' motion to dismiss is granted in part and denied in part. Plaintiffs are granted leave to replead within twenty-one (21) days.

It is so ordered.



MEDIDATA SOLUTIONS,  
INC., Plaintiff,

v.

FEDERAL INSURANCE  
CO., Defendant

15-CV-907 (ALC)

United States District Court,  
S.D. New York.

Signed 07/21/2017

**Background:** Insured corporation, which wired millions of dollars to unknown actor as a result of e-mail “spoofing” scheme, brought action against insurer, challenging insurer’s denial of insured’s claim under policy covering losses caused by certain criminal and fraudulent acts. Parties filed cross-motions for summary judgment.

**Holdings:** The District Court, Andrew L. Carter, Jr., J., held that:

- (1) insured’s losses were covered under computer fraud clause;
- (2) insured’s losses were covered under funds transfer fraud clause; and

- (3) insured’s losses were not covered by forgery clause.

Insured’s motion granted; insurer’s motion denied.

### 1. Insurance ⇨1806

Under New York law, insurance policies are interpreted according to general rules of contract interpretation.

### 2. Contracts ⇨147(1)

Under New York law, the fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties’ intent.

### 3. Contracts ⇨152

Under New York law, a written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms.

### 4. Contracts ⇨176(2)

Under New York law, when a contract is unambiguous, its interpretation is a question of law.

### 5. Insurance ⇨1817, 1822

In determining whether an insurance contract is ambiguous, a court applying New York law should focus on the reasonable expectations of the average insured upon reading the policy and employing common speech.

### 6. Insurance ⇨2153(1)

Under New York law, insured corporation’s losses stemming from e-mail “spoofing” scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation’s president, were covered under computer fraud clause in crime protection policy; scheme amounted to deceitful and dishonest access of insured’s computer system, as the fraud was

achieved by entry into insured's e-mail system with spoofed e-mails that used computer code to mask the thief's true identity, and while insured's employees took other steps before approving the wire transfer, the transfer was still the direct result of the spoofed e-mails.

#### 7. Insurance ⇨2153(1)

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were covered under funds transfer fraud clause in crime protection policy; given that the wire transfer depended on obtaining the consent of several high level employees by trick, the fact that insured's accounts payable employee willingly sent the transfer did not transform it into a valid transaction.

#### 8. Insurance ⇨2153(1)

Under New York law, insured corporation's losses stemming from e-mail "spoofing" scheme, which led insured to wire millions of dollars to unknown actor who posed as corporation's president, were not covered under forgery clause in crime protection policy; even if the spoofed e-mails constituted a forgery, the policy only covered forgeries or alterations of a financial instrument.

---

Adam Seth Ziffer, Robin L. Cohen, Alexander Michael Sugzda, McKool Smith, New York, NY, for Plaintiff

Christopher M. Kahler, Sara Gronkiewicz-Doran, Scott Schmookler, Gordon & Rees LLP, Chicago, IL, Jeffrey Yehuda Aria Spiegel, Joseph Salvo, Gordon & Rees, LLP, New York, NY, for Defendant

### MEMORANDUM AND ORDER GRANTING SUMMARY JUDGMENT

ANDREW L. CARTER, JR., District Judge:

Medidata Solutions, Inc. ("Medidata") commenced this action against Federal Insurance Company ("Federal") after Federal denied Medidata's claim for insurance coverage. The parties filed cross-motions for summary judgment and the Court ordered additional expert discovery. For the following reasons, Medidata's motion for summary judgment is GRANTED.

#### BACKGROUND

##### A. Medidata

Medidata provides cloud-based services to scientists conducting research in clinical trials. Medidata's Memorandum of Law in Support of Motion for Summary Judgment ("Pl's Mem.") at 3, ECF No. 37. Medidata used Google's Gmail platform for company emails. Affidavit of Glenn Watt in Support of Medidata's Motion for Summary Judgment, ("Watt Aff.") ¶ 2, ECF No. 39. Medidata email addresses consisted of an employee's first initial and last name followed by the domain name "mdsol.com" instead of "gmail.com". *Id.* ¶ 3. Email messages sent to Medidata employees were routed through Google computer servers. *Id.* ¶ 4. Google systems processed and stored the email messages. *Id.* ¶ 4. During processing, Google compared an incoming email address with Medidata employee profiles in order to find a match. *Id.* ¶ 9. If a match was found, Gmail displayed the sender's full name, email address, and picture in the "From" field of the message. *Id.* ¶¶ 8, 10, 11. After processing, the emails were displayed in the Medidata employee's email account. *Id.* ¶ 7. Medidata employees used computers owned by the company to

access the email messages that were processed and displayed by Google. *Id.*

### B. Fraud on Medidata

In the summer of 2014, Medidata notified its finance department of the company's short-term business plans which included a possible acquisition. Plaintiff's Rule 56.1 Statement ("Pl.'s 56.1") ¶ 36, ECF No. 36. Medidata instructed finance personnel "to be prepared to assist with significant transactions on an urgent basis." *Id.* ¶ 37. In 2014, Alicia Evans ("Evans") worked in accounts payable at Medidata. *Id.* ¶ 38. Evans was responsible for processing all of Medidata's travel and entertainment expenses. Joint Exhibit Stipulation ("Joint Ex. Stip.") Ex. 20, 41:16–21, ECF No. 41. On September 16, 2014, Evans received an email purportedly sent from Medidata's president. *Id.* Ex. 2. The email message contained the president's name, email address, and picture in the "From" field. *Id.* The message to Evans stated that Medidata was close to finalizing an acquisition, and that an attorney named Michael Meyer ("Meyer") would contact Evans. *Id.* The email advised Evans that the acquisition was strictly confidential and instructed Evans to devote her full attention to Meyer's demands. *Id.* Evans replied: "I will certainly assist in any way I can and will make this a priority." *Id.* Ex. 4.

On that same day, Evans received a phone call from a man who held himself out to be Meyer. *Id.* Ex. 20, 31:10–15. Meyer demanded that Evans process a wire transfer for him. *Id.* Meyer told Evans a physical check would not suffice because of time constraints. *Id.* Ex. 20, 36:5–8. Evans explained to Meyer that she needed an email from Medidata's president requesting the wire transfer. *Id.* Ex. 20, 34:17–20. Evans also explained she needed approval from Medidata Vice President Ho

Chin ("Chin"), and Director of Revenue Josh Schwartz ("Schwartz"). *Id.*

Chin, Evans, and Schwartz then received a group email purportedly sent from Medidata's president stating: "I'm currently undergoing a financial operation in which I need you to process and approve a payment on my behalf. I already spoke with Alicia, she will file the wire and I would need you two to sign off." *Id.* Ex. 6. The email contained the president of Medidata's email address in the "From" field and a picture next to his name. *Id.* In response, Evans logged on to Chase Bank's online system to initiate a wire transfer. *Id.* Ex. 20, 13:20–14:16. Evans entered the banking information provided by Meyer and submitted the wire transfer for approval. *Id.* Ex. 20, 15:11–23, 16:17–17:05. Schwartz and Chin logged on to Chase's online banking system and approved the wire transfer. *Id.* Ex. 21, 13:20–14:16; Ex. 19, 59:16–18, 60:02–04. \$4,770,226.00 was wired to a bank account that was provided by Meyer. *Id.* Ex. 8.

On September 18, 2014, Meyer contacted Evans requesting a second wire transfer. *Id.* Ex. 20, 42:02–10. Evans initiated the second wire transfer and Schwartz approved it. *Id.* Ex. 21, 40:24–41:20. However, Chin thought the email address in the "Reply To" field seemed suspicious. *Id.* Ex. 19, 46:08–24. Chin spoke with Evans about his suspicions and Evans composed a new email to Medidata's president inquiring about the wire transfers. *Id.* Ex. 20, 50:04–20. Medidata's president told Evans and Chin that he had not requested the wire transfers. *Id.* Medidata employees then realized that the company had been defrauded. *Id.* Ex. 19, 63:09–64:18. Medidata contacted the FBI and hired outside counsel to conduct an investigation. *Id.* The investigations revealed that an unknown actor altered the emails that were sent to Chin, Evans, and Schwartz to ap-

pear as if they were sent from Medidata's president. *Id.*

### C. Medidata Insurance Policy

Medidata held a \$5,000,000 insurance policy with Federal called "Federal Executive Protection". *Id.* Ex. 1. The Policy contained a "Crime Coverage Section" addressing loss caused by various criminal acts, including Forgery Coverage Insuring, Computer Fraud Coverage, and Funds Transfer Fraud Coverage. *Id.*

#### 1. Computer Fraud Coverage

The Policy's, "Computer Fraud Coverage", protected the "direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." *Id.* The Policy defined "Organization" as "any organization designated in Item 4 of the Declarations for this coverage section." *Id.* Item 4, in turn, lists "Medidat[a] Solutions, Inc., and its subsidiaries" as a covered Organization. *Id.* The Policy defined "Third Party" as "a natural person other than: (a) an Employee; or (b) a natural person acting in collusion with an Employee." *Id.*

The Policy defined "Computer Fraud" as: "[T]he unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." *Id.* A "Computer Violation" included both "the fraudulent: (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against an Organization." *Id.* The Policy defined "Data" broadly to include any "representation of information." *Id.* The Policy defined "Computer System" as "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are: (a) owned and operat-

ed by an Organization; (b) leased and operated by an Organization; or (c) utilized by an Organization." *Id.*

#### 2. Funds Transfer Fraud Coverage

The Policy's Funds Transfer Fraud Coverage protected "direct loss of Money or Securities sustained by an Organization resulting from Funds Transfer Fraud committed by a Third Party." *Id.* The Policy defined "Funds Transfer Fraud" as: "fraudulent electronic . . . instructions . . . purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent." *Id.*

#### 3. Forgery Coverage

The Policy's Forgery Coverage protected "direct loss sustained by an Organization resulting from Forgery or alteration of a Financial Instrument committed by a Third Party". *Id.* "Forgery" is defined as "the signing of the name of another natural person . . . with the intent to deceive . . . Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." *Id.*

#### 4. Claim For Coverage

On September 25, 2014, Medidata submitted a claim to Federal requesting coverage of the fraud under three clauses. *Id.* Ex. 11. Federal assigned regional claims technician Michael Maillet ("Maillet") to investigate the fraud on Medidata. *Id.* Ex. 12.

On December 24, 2014, Federal denied Medidata's claim for coverage. *Id.* Federal denied coverage under the computer fraud clause, because there had been no "fraudulent entry of Data into Medidata's computer system." *Id.* at 4. As support, Federal

explained that [t]he subject emails containing false information were sent to an inbox which was open to receive emails from any member of the public” thus the entry of the fictitious emails “was authorized.” *Id.* In addition, Federal concluded that there had been no “change to data elements” because the emails did not cause any fraudulent change to data elements or program logic of Medidata’s computer system. *Id.* Federal conceded that Gmail added the name and picture of Medidata’s president because of the email, however, Federal stated that the fake email did not cause this to happen. *Id.* According to Federal, Medidata’s computer system, “populated the email in the normal manner.” *Id.* at 5.

Federal denied coverage under the funds transfer fraud clause because the wire transfer had been authorized by Medidata employees and thus was made with the knowledge and consent of Medidata. *Id.*

Finally, Federal rejected Medidata’s claim for Forgery Coverage because the emails did not contain an actual signature and did not meet the Policy’s definition of a Financial Instrument. *Id.* Federal also based its denial of both the Forgery Coverage and the Computer Fraud Coverage claims on the belief that the emails did not directly cause Medidata’s loss, because no loss would have taken place if Medidata employees had not acted on the instructions contained in those emails. *Id.*

On January 13, 2015, Medidata sent a letter responding to the denial and setting forth the basis for coverage under the Policy. *Id.* Ex. 14. Federal replied on January 30, 2015, reasserting its denial of coverage for the claim. *Id.* Ex. 15.

### DISCUSSION

Summary judgment is appropriate where “the pleadings, depositions, answers to interrogatories and admissions on file,

together with affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 322, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986); *see also* Fed. R. Civ. P. 56(c). “There is no issue of material fact where the facts are irrelevant to the disposition of the matter.” *Chartis Seguros Mexico, S.A. de C.V. v. HLI Rail & Rigging, LLC*, 967 F.Supp.2d 756, 761 (S.D.N.Y. 2013). “Speculation, conclusory allegations and mere denials are not enough to raise genuine issues of fact.” *Id.* (citing *National Union Fire Ins. Co. of Pittsburgh, Pa. v. Walton Ins. Ltd.*, 696 F.Supp. 897, 900 (S.D.N.Y. 1988)).

The burden lies with the moving party to demonstrate the absence of any genuine issue of material fact and all inferences and ambiguities are to be resolved in favor of the nonmoving party. *See Celotex Corp.*, 477 U.S. at 323, 106 S.Ct. 2548 (1986); *see also Hotel Emps. & Rest. Emps. Union, Local 100 v. City of New York Dep’t of Parks & Recreation*, 311 F.3d 534, 543 (2d Cir. 2002). If “no rational jury could find in favor, of the nonmoving party because the evidence to support its case is so slight, there is no genuine issue of material fact and a grant of summary judgment is proper.” *Gallo v. Prudential Residential Servs., Ltd. P’ship*, 22 F.3d 1219, 1224 (2d Cir. 1994). An identical standard applies where the parties file cross-motions for summary judgment: “each party’s motion must be examined on its own merits, and in each case all reasonable inferences must be drawn against the party whose motion is under consideration.” *Morales v. Quintel Entm’t, Inc.*, 249 F.3d 115, 121 (2d Cir. 2001) (citation omitted).

[1–5] Under New York law, insurance policies are interpreted according to general rules of contract interpretation. *Olin*

*Corp. v. Am. Home Assur. Co.*, 704 F.3d 89, 98 (2d Cir. 2012). “The fundamental, neutral precept of contract interpretation is that agreements are construed in accord with the parties’ intent. . . . [A] written agreement that is complete, clear and unambiguous on its face must be enforced according to the plain meaning of its terms.” *Bank of New York v. First Millennium, Inc.*, 598 F.Supp.2d 550, 556 (S.D.N.Y. 2009) *aff’d*, 607 F.3d 905 (2d Cir. 2010) (citing *Greenfield v. Philles Records, Inc.*, 98 N.Y.2d 562, 569, 750 N.Y.S.2d 565, 780 N.E.2d 166 (2002)). When a contract is unambiguous, its interpretation is a question of law. *See 82–11 Queens Blvd. Realty, Corp. v. Sunoco, Inc. (R & M)*, 951 F.Supp.2d 376, 381 (E.D.N.Y. 2013). In determining whether an insurance contract is ambiguous, a Court should focus “on the reasonable expectations of the average insured upon reading the policy and employing common speech.” *Universal Am. Corp. v. Nat’l Union Fire Ins. Co.*, 25 N.Y.3d 675, 680, 16 N.Y.S.3d 21, 37 N.E.3d 78 (2015).

#### A. Computer Fraud Coverage

[6] Medidata argues that the Policy’s Computer Fraud clause covers the company’s loss in 2014, because a thief fraudulently entered and changed data in Medidata’s computer system. Pl.’s Mem. at 14–20. Specifically, Medidata asserts that the address in the “From” field of the spoofed emails constituted data which was entered by the thief posing as Medidata’s president. *Id.* at 14. Also, a thief entered a computer code which caused Gmail to

“change” the hacker’s email address to the Medidata president’s email address. *Id.* at 19–20.

Federal argues that Medidata’s loss in 2014 is not covered by the Computer Fraud clause, because the emails did not require access to Medidata’s computer system, a manipulation of those computers, or input of fraudulent information. Federal’s Memorandum of Law in Support of Summary Judgment (“Def’s Mem.”) at 9–12, ECF No. 34. The Court has reviewed the Policy and concludes that, as a matter of law, the unambiguous language of the Computer Fraud clause provides coverage for the theft from Medidata.

Under Medidata’s policy, a computer violation occurs upon the “the fraudulent: (a) entry of Data into or deletion of Data from a Computer System” or “(b) change to Data elements or program logic of a Computer System, which is kept in machine readable format.” The New York Court of Appeals shed light on these phrases in *Universal*, which involved a health insurance company that was defrauded by healthcare providers who entered claims for reimbursement of services that were never rendered. 25 N.Y.3d at 681–82, 16 N.Y.S.3d 21, 37 N.E.3d 78.<sup>1</sup> *Universal* sought insurance coverage for the losses incurred by the fraudulent claims. *Id.* at 679, 16 N.Y.S.3d 21, 37 N.E.3d 78. *Universal*’s computer fraud clause covered “loss resulting directly from a fraudulent entry of Electronic Data or Computer Program into, or change of Electronic Data or Computer Program within” the insured’s computer system.”

1. The trial court noted “the perpetrators enrolled new members in the . . . plan with the person’s cooperation, in return for which the member received a kickback from the provider. In some cases, the provider used the member’s personal information without that person’s knowledge. In either event, the provider itself did not enroll in the plan. Instead, they

were able to submit claims after obtaining a National Provider Identifier (NPI) from [the agency of the U.S. Department of Health and Human Service tasked with overseeing this market]. In some cases, the NPI was obtained for a fictitious provider, in other cases it was fraudulently taken from a legitimate provider.”

*Id.* In denying coverage, the Court of Appeals held that the unambiguous language of Universal's policy "applie[d] to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users." *Id.* at 680–81, 16 N.Y.S.3d 21, 37 N.E.3d 78. The court reasoned that the drafter's "intentional placement of 'fraudulent' before 'entry' and 'change' manifest[ed] the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access." *Id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78.

Here, the fraud on Medidata falls within the kind of "deceitful and dishonest access" imagined by the New York Court of Appeals. *Id.* It is undisputed that the theft occurred by way of email spoofing.<sup>2</sup> Joint Factual Stipulation Following Discovery ("Joint Fact Stip.") ¶ 7, ECF 72. To that end, the thief constructed messages in Internet Message Format ("IMF") which the parties compare to a physical letter containing a return address. *Id.* ¶ 2. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). *Id.* ¶ 1. Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. *Id.* To mask the true origin of the spoofed emails, the thief embedded a computer code. *Id.* ¶ 10. The computer code caused the SMTP Envelope and the IMF Letter to display different email addresses in the "From" field. *Id.* The spoofed emails showed the thief's true email address in the SMTP "From" field, and Medidata's

president's email address in the IMF "From" field. *Id.* ¶¶ 20–21. When Gmail received the spoof emails, the system compared the address in the IMF "From" field with a list of contacts and populated Medidata's president's name and picture. *Id.* ¶ 15. The recipients of the Gmail messages only saw the information in the IMF "From" field. *Id.* ¶ 11.

Federal's reading of *Universal* is overbroad. In this case, Federal focuses on the thief's construction of the spoofed emails and computer code before sending them to Gmail, arguing that, as a result, there was no entry or change of data to Medidata's computer system. Def's Mem. at 9–12. Under this logic, *Universal* would require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage. However, this reading of *Universal* incorrectly limits the coverage of the policy in this case. It is true that the Court of Appeals in *Universal* peppered its opinion with references to hacking as the example for a covered violation. *See e.g., id.* at 681, 16 N.Y.S.3d 21, 37 N.E.3d 78 ("[T]he the rider covers losses from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be 'hacking' of the computer system."). But a hacking is one of many methods a thief can use, and "is an everyday term for unauthorized access to a computer system." *Dial Corp. v. News Corp.*, No. 13-CV-6802, 2016 WL 690868, at \*3 (S.D.N.Y. Feb. 17, 2016) (citation omitted). Thus, *Universal* is more appropriately read as finding coverage for fraud where the perpetrator violates the

2. A court in this district defined "Spoofing" as "the practice of disguising a commercial e-mail to make the e-mail appear to come from an address from which it actually did not originate. Spoofing involves placing in the "From" or "Reply-to" lines, or in other portions of e-mail messages, an e-mail address

other than the actual sender's address, without the consent or authorization of the user of the e-mail address whose address is spoofed." *Karvaly v. eBay, Inc.*, 245 F.R.D. 71, 91 n.34 (E.D.N.Y. 2007) (citation and internal quotation marks omitted).



integrity of a computer system through unauthorized access and denying coverage for fraud caused by the submission of fraudulent data by authorized users. *Id.* (noting “[o]ther language in the rider confirms that the rider seeks to address unauthorized access”). Indeed, an examination of the trial court’s analysis in *Universal* further emphasizes this point. The N.Y. Supreme Court held Universal’s policy “indicates that coverage is for an unauthorized entry into the system, i.e. by an unauthorized user, such as a hacker, or for unauthorized data, e.g. a computer virus.” The trial court was also concerned with unauthorized users and corrupting data instead of authorized users submitting untruthful content.<sup>3</sup> *Id.* (“Nothing in this clause indicates that coverage was intended where an authorized user utilized the system as intended, i.e. to submit claims, but not where the claims themselves were fraudulent.”).

Federal’s reliance on *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, is also misplaced. The court in *Pestmaster*, held that a corporation’s computer fraud insurance policy did not cover a theft by the company’s payroll administrator, because the administrator was authorized to withdraw funds from the corporation’s bank account, notwithstanding the fact that he later misappropriated the payroll funds. No. 13-CV-5039 (JFW), 2014 WL 3844627, at \*6 (C.D. Cal. July 17, 2014). Relying on *Universal*, the Court explained that “Computer Fraud occurs when someone hacks or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds.” *Id.* (internal quotation marks

omitted). In contrast, the fraud on Medidata was achieved by entry into Medidata’s email system with spoofed emails armed with a computer code that masked the thief’s true identity. The thief’s computer code also changed data from the true email address to Medidata’s president’s address to achieve the email spoof.

In challenging causation, Federal contends that “there is no direct nexus” between the spoofed emails and the fraudulent wire transfer. Defs Mem. at 13–15. According to Federal, the spoofed emails “did not create, authorize, or release a wire transfer” because Medidata employees received telephone calls from the thief and took other steps in approving the fraudulent transfer. *Id.* at 16. As support, Federal cites to the Fifth Circuit’s decision in *Apache Corp. v. Great American Ins. Co.* denying coverage of a similarly worded computer fraud provision. 662 Fed.Appx. 252 (5th Cir. 2016). The underlying fraud in *Apache* was achieved through a muddy chain of events. The insured was duped into sending payments to thieves that were intended for the insured’s vendor. *Id.* at 253. The thieves engaged in a concerted effort to achieve the fraud which included phone calls, spoofed emails, and falsified documents. *Id.* Applying Texas law, the Fifth Circuit held that the insured’s computer fraud provision did not cover the theft because “the fraudulent transfer was the result of other events and not directly by the computer use.” *Id.* The Court explained that the insured “invited the computer-use at issue . . . even though the computer-use was but one step in Apache’s multi-step, but flawed, process that ended in its making required and authorized,

3. The Appellate Division appeared to have a similar concern when it found that the language of the policy “was intended to apply to wrongful acts in manipulation of the computer system, i.e., by hackers, and did not pro-

vide coverage for fraudulent content consisting of claims by bona fide doctors and other health care providers authorized to use the system for reimbursement for health care services that were not provided.”

very large invoice payments, but to a fraudulent bank account.” *Id.* at 258–59. In contrast, Medidata employees did not invite the spoofed emails at issue. The chain of events began with an accounts payable employee receiving a spoofed email from a person posing as Medidata’s president. To the extent that the facts of this case fit within *Apache*, the Court finds its causation analysis unpersuasive. The Court finds that Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata’s president.

Federal also cites to the Ninth Circuit’s decision in *Taylor & Lieberman v. Federal Ins. Co.*, denying coverage of a computer fraud provision. (“*Taylor I*”), 681 Fed. Appx. 627, 628 (9th Cir. 2017). In *Taylor*, an accounting firm fell victim to an email spoofing scam after a thief invaded the email account of the accounting firm’s client. *Id.* at 628. The thief, disguised as the client, sent emails requesting wire transfers to a specified bank account. *Id.* The district court keenly pointed out the “series of far more remote circumstances” than simply a theft directly from the accounting firm. *Taylor & Lieberman v. Fed. Ins. Co.*, No. 14-CV-3608 (RSWL) (SHX), 2015 WL 3824130, at \*4 (C.D. Cal. June 18, 2015) (“*Taylor II*”). The district court emphasized that the thief stole money from the client not the accounting firm, and that the accounting firm was seeking reimbursement for the loss of its client’s money. *Id.* at \*4. Importantly, the court added, “if the funds had been held in an account owned or attributed to Plaintiff, such as an escrow account and a hacker had entered into Plaintiff’s computer system . . . then Plaintiff would be correct in asserting coverage from the Policy.” *Id.* The Ninth Circuit agreed, noting that the mere sending of emails from the client to the accounting firm did not constitute unauthorized entry into the accounting firm’s computer sys-

tem. *Taylor I*, 681 Fed.Appx. at 629–30. But Medidata did not suffer a loss from spoofed emails sent from one of its clients. A thief sent spoofed emails armed with a computer code into the email system that Medidata used. Also, the fraud caused transfers out of Medidata’s own bank account. Therefore, Medidata was “correct in asserting coverage from the Policy.” *Taylor II*, 2015 WL 3824130, at \*4.

Accordingly, Medidata has demonstrated that its losses were a direct cause of a computer violation.

### B. Funds Transfer Fraud Coverage

[7] Medidata argues that it was improperly denied coverage under the Funds Transfer Fraud clause because the theft in 2014 “(1) caused a direct loss of money; (2) by fraudulent electronic instructions purportedly issued by Medidata; (3) issued to a financial institution; (4) to deliver money from Medidata’s accounts; (5) without Medidata’s knowledge or consent.” PI’s Mem. at 20. Federal challenges the last of the requisite elements, arguing that the bank wire transfer in 2014 was voluntary and with Medidata’s knowledge and consent. Def’s Mem. at 21–24. Federal also argues that, because Medidata employees voluntarily transferred the money, it was actually issued by Medidata instead of “purportedly issued” as the Policy demands. *Id.* at 24–25. The Court finds that the unambiguous language of the Policy covers the theft from Medidata in 2014.

The Policy defines Funds Transfer Fraud as: “fraudulent electronic . . . instructions . . . purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization’s knowledge or consent.”

Joint Ex. Stip., Ex. 1. Under *Pestmaster*, which Federal relies, a funds transfer fraud agreement, “does not cover authorized or valid electronic transactions . . . even though they are, or maybe, associated with a fraudulent scheme.” 2014 WL 3844627, at \*5. However, *Pestmaster* involved a corporation that made several valid electronic transfers to its payroll administrator who later misappropriated the funds. *Id.* at \*6. The court justified the denial of coverage by pointing out, “there is no evidence that . . . any third party, gained unauthorized entry into Pestmaster’s bank’s electronic fund transfer system **or pretended to be an authorized representative** or otherwise altered the electronic instructions in order to wrongfully divert money from the rightful recipient.” *Id.* (emphasis added). Also unpersuasive is Federal’s reliance on *Cumberland Packing Corp. v. Chubb Ins. Corp.*, which interpreted a funds transfer fraud agreement. 29 Misc.3d 1208(A), 2010 WL 3991185, at \*5 (Sup. Ct. 2010). The court in *Cumberland* denied coverage to a policyholder who had voluntarily transferred funds to Bernie Madoff for investment purposes. *Id.* The court reasoned that “Madoff was expressly authorized to act as plaintiffs’ broker/agent” which did not involve unauthorized instructions to transfer money. *Id.* In this case, it is undisputed that a third party masked themselves as an authorized representative, and directed Medidata’s accounts payable employee to initiate the electronic bank transfer. It is also undisputed that the accounts payable personnel would not have initiated the wire transfer, but for, the third parties’ manipulation of the emails. The fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees’ knowl-

edge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny. Therefore, Medidata has demonstrated that the Funds Transfer Fraud clause covers the theft in 2014.

### C. Forgery Coverage

[8] The theft from Medidata in 2014 does not trigger coverage under the Forgery clause, because the Policy requires a “direct loss resulting from Forgery or alteration of a Financial Instrument committed by a Third Party.” Joint Ex. Stip., Ex. 1. The parties vehemently dispute whether the spoofed emails containing Medidata’s president’s name constitute a forgery. *See* Pl’s Mem. at 18; Def’s Mem. at 17. However, the Court need not resolve the matter. Even if the emails contained a forgery, the absence of a financial instrument proves fatal to Medidata’s claim for coverage. In a strained reading of the Policy, Medidata argues that a forgery itself triggers coverage even in the absence of a financial instrument. Medidata’s Memorandum of law in Further Support of Summary Judgment (“Pl’s Reply”) at 20, ECF No. 52. However, “[t]he entire contract must be reviewed and particular words should be considered, not as if isolated from the context, but in the light of the obligation as a whole and the intention of the parties as manifested thereby. Form should not prevail over substance and a sensible meaning of words should be sought.” *Riverside S. Planning Corp. v. CRP/Extell Riverside, L.P.*, 13 N.Y.3d 398, 404, 892 N.Y.S.2d 303, 920 N.E.2d 359 (2009) (citations, alterations, and internal quotation marks omitted). Medidata’s interpretation of the Policy would render the word forgery vague and create ambiguity in the clause. To the contrary, a forgery or alteration are both means by which a person can corrupt a financial instrument resulting in a loss to

the insured. If forgery is viewed in isolation, the Policy would certainly be converted to a general crime policy. Therefore, Medidata has not demonstrated that it suffered a loss that was covered by the Forgery clause.

### CONCLUSION

For the foregoing reasons, Medidata's motion for summary judgment is **GRANTED** and Federal's motion for summary judgment is **DENIED**.

**SO ORDERED.**



**J.T. MAGEN & COMPANY,  
INC., Plaintiff,**

**v.**

**ALLEN EDMONDS CORP., Defendant.**

**15 Civ. 8620 (LLS)**

United States District Court,  
S.D. New York.

Signed 06/23/2017

Filed 06/26/2017

**Background:** Contractor brought action against store owner for breach of contract, quantum meruit and account stated, seeking to recover monies owed for general construction work performed at store. Contractor moved for summary judgment.

**Holdings:** The District Court, Louis L. Stanton, J., held that:

- (1) genuine issue of material fact precluded summary judgment on contractor's breach of contract claim against owner, and

- (2) genuine issue of material fact precluded summary judgment on contractor's account stated claim.

Motion denied.

### 1. Federal Civil Procedure $\S$ 2470.1

On a motion for summary judgment, a fact is "material" if it might affect the outcome of the suit under the governing law, and a dispute is "genuine" if the evidence is such that a reasonable jury could return a verdict for the nonmoving party. Fed. R. Civ. P. 56(a).

See publication Words and Phrases for other judicial constructions and definitions.

### 2. Federal Civil Procedure $\S$ 2543

In looking at the record, on a motion for summary judgment, the court construes the evidence in the light most favorable to the nonmoving party and draws all inferences and resolves all ambiguities in favor of the nonmoving party. Fed. R. Civ. P. 56(a).

### 3. Judgment $\S$ 181(19)

Genuine issue of material fact as to whether relationship between store owner and contractor, in relation to general construction work performed at store, was that of owner and general contractor, such that contractor could recover monies owed from owner, precluded summary judgment on contractor's breach of contract claim against owner.

### 4. Federal Civil Procedure $\S$ 2552

A motion for summary judgment does not entitle a court to try issues of fact; its function is limited to deciding whether there are any such issues to be tried. Fed. R. Civ. P. 56(a).

### 5. Pleading $\S$ 53(2)

Under New York law, where the existence of a contract is in dispute, the plaintiff may allege a cause of action to recover

2016 WL 4618761

Only the Westlaw citation is currently available.

United States District Court,  
N.D. Georgia, Atlanta Division.

Principle Solutions Group, LLC, Plaintiff,

v.

Ironshore Indemnity, Inc., Defendant.

CIVIL ACTION NO. 1:15-CV-4130-RWS

|

Signed 08/30/2016

**Attorneys and Law Firms**

Carrie Marie Raver, Barnes & Thornburg, Fort Wayne, IN, James J. Leonard, Barnes & Thornburg LLP, Atlanta, GA, Scott N. Godes, Barnes & Thornburg, LLP, Washington, DC, for Plaintiff.

Amanda Dawn Proctor, Philip Wade Savrin, Freeman Mathis & Gary, LLP, Atlanta, GA, for Defendant.

**ORDER**

**RICHARD W. STORY**, United States District Judge

\*1 This matter is before the Court on Plaintiff's Motion for Partial Summary Judgment [Doc. No. 22], Defendant's Motion for Summary Judgment [Doc. No. 32], Plaintiff's Motion to Exclude [Doc. No. 38], and Plaintiff's Motion for Judicial Notice [Doc. No. 39].

**I. Factual Background**

This is an insurance dispute in which Plaintiff Principle Solutions Group ("Principle") seeks payment of \$1.717 million from its insurer, Defendant Ironshore Indemnity ("Ironshore").

On July 8, 2015, Principle was the victim of a fraud scheme. At 9:10am that day, Principle's controller received an email from a person purporting to be Josh Nazarian, one of the managing directors for Principle [Doc. No. 22-7, ¶ 2, admitted; Doc. No. 22-3, p. 6]. The email appeared to have been sent

from his corporate email address [Id.]. The email referenced a company acquisition and instructed the controller to "treat the matter with the utmost discretion" [Doc. No. 22-7, ¶ 3, admitted; Doc. No. 22-3, p. 6]. The email also instructed the controller to work with an attorney, Mark Leach, to "ensure that the wire goes out today" [Id.]. Mr. Nazarian was not in the office on the day of the fraudulent email [Doc. No. 22-7, ¶ 4, admitted]. He did not send the email [Doc. No. 22-7, ¶ 5, admitted].

Later that morning, the controller received an email from a "Mark Leach" who represented himself to be a partner at Alston & Bird [Doc. No. 22-7, ¶ 6, admitted; Doc. No. 22-3, p. 9]. Mr. Leach stated that he was reaching out at the request of Mr. Nazarian [Id.]. Mr. Leach also sent wiring instructions to a bank in China [Id., Doc. No. 22-3, p. 11]. At 10:15am, Mr. Leach called the controller and emphasized that they needed to complete the wire transaction that day and that he had Mr. Nazarian's full approval to execute the wire [Doc. No. 22-7, ¶ 8, admitted].

The controller was not able to forward an email to the financial institution to wire the funds because the institution required more than an email to wire funds from an account [Doc. No. 22-7, ¶ 9, admitted]. So, the controller logged into the company's online account to enable the approval function and to verify the capability to wire internationally in different forms of currency [Doc. No. 22-7, ¶ 10, admitted]. She then called Mr. Leach to confirm the capability and instructed another Principle employee to create the wire instructions [Doc. No. 22-7, ¶ 11, admitted]. The controller then approved the wire [Doc. No. 22-7, ¶ 12, admitted].

The financial institution's fraud prevention unit called and emailed the controller requesting verification of the wire [Doc. No. 22-7, ¶ 13, admitted]. The financial institution requested the controller to verify how Mr. Leach had received the wire instructions [Doc. No. 22-7, ¶ 14, admitted]. The controller called Mr. Leach and was told he verbally received the wire instructions from Mr. Nazarian [Doc. No. 22-7, ¶ 15, admitted]. The controller relayed this information to the financial

institution, and the financial institution released the wire [Doc. No. 22-7, ¶ 16, admitted].

\*2 The next day, the controller spoke with Mr. Nazarian and told him that the wire had been made in accordance with his instruction [Doc. No. 22-7, ¶ 17, admitted]. Mr. Nazarian had no knowledge of the emails, Mr. Leach, or the wire instructions, and he immediately called the fraud department of the financial institution to report the fraud [Doc. No. 22-7, ¶ 18, admitted]. Neither the financial institution nor law enforcement were able to recover the funds [Doc. No. 22-7, ¶ 19, admitted]. Principle suffered a \$1.717 million loss [Doc. No. 22-7, ¶ 20, admitted].

Principle is the named insured under Commercial Crime Policy No. 001512502 for the policy period of December 20, 2014 to December 20, 2015 [Doc. No. 22-7, ¶ 21, admitted]. Principle paid the premium for the Commercial Crime Policy [Doc. No. 22-7, ¶ 22, admitted]. The Commercial Crime Policy provides coverage for specifically-defined categories of crimes, one of which is “Computer and Funds Transfer Fraud” [Doc. No. 22-7, ¶ 23, admitted]. The “Limit of Insurance” is \$5,000,000 per occurrence with a \$25,000 deductible per occurrence [*Id.*].

Specifically, Section A.6 of the Commercial Crime Policy states:

a. We will pay for:

- (2) Loss resulting directly from a “fraudulent instruction” directing a “financial institution” to debit your “transfer account” and transfer, pay or deliver “money” or “securities” from that account.

[Doc. No. 22-4, p. 7]. The Commercial Crime Policy further provides various definitions in Section F, including the following:

9. “Financial institution” means:

b. With regard to Insuring Agreement A.6:

- (1) A bank, savings bank, savings and loan association, trust company, credit union or similar depository institution;

(2) An insurance company; or

(3) A stock brokerage firm or investment company.

12. “Fraudulent instruction” means:

a. With regard to Insuring Agreement A.6.a. (2):

(1) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instruction directing a “financial institution” to debit your “transfer account” and to transfer, pay or deliver “money” or “securities” from that “transfer account”, which instruction purports to have been issued by you, but which in fact was fraudulently issued by someone else without your knowledge or consent.

(2) A written instruction (other than those covered by Insuring Agreement A.2.) issued to a “financial institution” directing the “financial institution” to debit your “transfer account” and to transfer, pay or deliver “money” or “securities” from that “transfer account”, through an electronic funds transfer system at specified times or under specified conditions, which instruction purports to have been issued by you, but which in fact was issued, forged or altered by someone else without your knowledge or consent.

(3) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or written instruction initially received by you, which instruction purports to have been issued by an “employee”, but which in fact was fraudulently issued by someone else without your or the “employee’s” knowledge or consent.

16. “Money” means:

a. Currency, coins and bank notes in current use and having a face value;

b. Traveler’s checks and money orders held for sale to the public; and

c. In addition, includes:

- (1) Under Insuring Agreements A.1. and A.2., deposits in your account at any financial institution; and
- (2) Under Insuring Agreement A.6., deposits in your account at a “financial institution” as defined in Paragraph F.9.b.

[Doc. No. 22-4, pp. 16-19].

Principle notified Ironshore of its claim consistent with the terms of the Policy [Doc. No. 22-7, ¶ 26, admitted]. Thereafter, Principle submitted a Sworn Proof of Loss to Ironshore under the Commercial Crime Policy, which it later amended, seeking coverage under the Commercial Crime Policy [Doc. No. 22-7, ¶ 27, admitted]. Ironshore denied coverage for the claim on July 24, 2015 [Doc. No. 22-7, ¶ 29, admitted].

**\*3** On October 20, 2015, Principle filed this action in the Superior Court of Fulton County, Georgia [Doc. No. 1-2]. The action was removed to this Court on November 25, 2015, based on this Court's diversity jurisdiction. The Complaint alleges claims for Breach of Contract and Bad Faith pursuant to [O.C.G.A. § 33-4-6](#) [Doc. No. 1-2].

## II. Plaintiff's Motion to Exclude [Doc. No. 38]

Plaintiff Principle has moved the Court to exclude Exhibit 2 [Doc. Nos. 30-2 and 32-4], which was submitted by Ironshore in support of its summary judgment briefing. Principle contends that Ironshore has failed to properly authenticate the document. Principle also contends that Exhibit 2 should be excluded because it is not relevant, and even if it was, it should be excluded pursuant to [Federal Rule of Evidence 403](#). Finally, Principle contends that the document was not properly provided according to Local Rule 56.1.

Exhibit 2 is a document that purports to be an endorsement and is titled “Add Cyber Deception Coverage.” Ironshore argues that this exhibit is provided as an illustration of the type of policy language which may provide coverage for this type of claim and that it is merely an aid for the Court

in construing the Policy language. The Court agrees with Principle that Exhibit 2 is not relevant. The endorsement is not part of the Policy at issue in this case. Also, it appears to be dated March 2015, and there is no evidence that Ironshore has sought or received approval from the Georgia Department of Insurance to use the endorsement in Georgia. It is not relevant to determining coverage under this Policy and is not relevant to the coverage issued raised by the parties. As such, Plaintiff's Motion to Exclude [Doc. No. 38] is GRANTED.

## III. Plaintiff's Motion for Judicial Notice [Doc. No. 39]

Plaintiff Principle has moved the Court to take judicial notice of certain filings made with the Georgia Department of Insurance [Doc. No. 39]. Specifically, Principle requests that the Court take judicial notice of the following facts: (1) Form SURE-130089150 was drafted by The Surety & Fidelity Association of America and was filed with the Georgia Department of Insurance because it was located in the Department's SERFF database; and (2) Ironshore's Exhibit 2 [Doc. Nos. 30-2 and 32-4] was not filed with the Georgia Department of Insurance because it cannot be located in their SERFF database.

As to the first fact, Ironshore does not oppose Plaintiff's Motion, and Plaintiff's Motion [Doc. No. 39] is GRANTED as to that fact. The Court will take judicial notice that Form SURE-130089150 was drafted by The Surety & Fidelity Association of America and was filed with the Georgia Department of Insurance. The Court also takes judicial notice of its contents.

As to the second fact, Ironshore contends that this fact is not relevant to any issue in this case. As discussed above, the Court agrees. The cyber-deception endorsement is not a part of the Commercial Crime Policy issued by Ironshore to Principle. Accordingly, whether or not the endorsement has been filed or approved for use in Georgia is irrelevant to the issue of whether the Policy covered the loss in this case. As to the second fact, Plaintiff's Motion [Doc. No. 39] is DENIED.



For the reasons stated above, Plaintiff's Motion for Judicial Notice [Doc. No. 39] is GRANTED in part and DENIED in part. The Court will take judicial notice of the first fact but not the second.

#### IV. Motions for Summary Judgment [Doc. Nos. 22 and 32]

\*4 The parties have filed cross-motions for summary judgment regarding the scope of the insurance coverage at issue. The material facts of the case outlined above are agreed upon by the parties, so there are no issues of material fact. Thus, a legal determination is needed as to whether the fraud in question is covered by the Policy.

##### A. Legal Standard

Federal Rule of Civil Procedure 56 requires that summary judgment be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(a). "The moving party bears 'the initial responsibility of informing the ... court of the basis for its motion, and identifying those portions of the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, which it believes demonstrate the absence of a genuine issue of material fact.'" Hickson Corp. v. N. Crossarm Co., 357 F.3d 1256, 1259 (11th Cir. 2004) (quoting Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986) (internal quotations omitted)). Where the moving party makes such a showing, the burden shifts to the non-movant, who must go beyond the pleadings and present affirmative evidence to show that a genuine issue of material fact does exist. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 257 (1986). The applicable substantive law identifies which facts are material. Id. at 248. A fact is not material if a dispute over that fact will not affect the outcome of the suit under the governing law. Id. An issue is genuine when the evidence is such that a reasonable jury could return a verdict for the non-moving party. Id. at 249-50.

In resolving a motion for summary judgment, the court must view all evidence and draw all reasonable inferences in the light most favorable to the non-moving party. Patton v. Triad Guar. Ins.

Corp., 277 F.3d 1294, 1296 (11th Cir. 2002). But, the court is bound only to draw those inferences that are reasonable. "Where the record taken as a whole could not lead a rational trier of fact to find for the non-moving party, there is no genuine issue for trial." Allen v. Tyson Foods, Inc., 121 F.3d 642, 646 (11th Cir. 1997) (quoting Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986)). "If the evidence is merely colorable, or is not significantly probative, summary judgment may be granted." Anderson, 477 U.S. at 249-50 (internal citations omitted); see also Matsushita, 475 U.S. at 586 (once the moving party has met its burden under Rule 56(a), the nonmoving party "must do more than simply show there is some metaphysical doubt as to the material facts").

##### B. Analysis – Coverage

Principle contends that the loss at issue is covered by Section A.6.a.(2). of the Commercial Crime Policy which provides coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer, pay or deliver 'money' or 'securities' from that account." Principle argues that its loss resulted directly from the fraudulent email that appeared to have been sent by Mr. Nazarian. In support of its denial of coverage, Ironshore argues that the loss did not result "directly" because: (1) additional information for the wire was conveyed to Principle by Mr. Leach after the initial email, and (2) Principle's employees set up and approved the wire transfer.

\*5 The Court finds that the language of the provision at issue is ambiguous. "When the language of an insurance contract is ambiguous and subject to more than one reasonable construction, the policy must be construed in the light most favorable to the insured, which provides him with coverage." Western Pacific Mut. Ins. Co. v. Davies, 601 S.E.2d 363, 369 (Ga. Ct. App. 2004). It is reasonable for Plaintiff to interpret the language of the policy to provide coverage even if there were intervening events between the fraud and the loss. Defendant's interpretation, which would require an immediate link between the injury and its cause, is also reasonable. In this circumstance, the Court must construe the policy in the light most



favorable to Plaintiff and provide coverage. This is consistent with the District Court's decision in [Apache Corp. v. Great Am. Ins. Co.](#), Civil Action No. 4:14-CV-237, 2015 WL 7709584, at \*3 (S.D. Texas Aug. 7, 2015), in which the Court stated that adopting the insurance company's reading would be “to limit the scope of the policy to the point of almost non-existence.” As in [Apache](#), Plaintiff here could act only through its officers and employees. If some employee interaction between the fraud and the loss was sufficient to allow Defendant to be relieved from paying under the provision at issue, the provision would be rendered “almost pointless” and would result in illusory coverage. *Id.*

As to coverage, Plaintiff's Motion for Partial Summary Judgment [Doc. No. 22] is GRANTED, and Defendant's Motion for Summary Judgment [Doc. No. 32] is DENIED as moot.

### C. Analysis – Bad Faith

Defendant has also moved for summary judgment as to Plaintiff's bad faith claim. O.C.G.A. § 33-4-6 provides the exclusive remedy for an insured's bad faith refusal to pay insurance proceeds. [Great Southwest Express Co. v. Great Am. Ins. Co.](#), 665 S.E.2d 878 (Ga. Ct. App. 2008). For Plaintiff to prevail on a claim for bad faith, it must prove: (1) that the claim is covered under the Policy; (2) that a demand for payment was made against the insurer within 60 days prior to filing suit; and (3) that the insurer's failure to pay was motivated by bad faith. [Lawyers Title Ins. Co. v. Griffin](#), 691 S.E.2d 633, 636 (Ga. Ct. App. 2010) (citation omitted).

To determine whether the insurer engaged in bad faith, an insured must show by evidence that “under the terms of the policy upon which the demand is made and under the facts surrounding the response to that demand, the insurer had no ‘good cause’ for resisting and delaying payment.” *Id.* (citing [Georgia Intl. Life Ins. Co. v. Harden](#), 280 S.E.2d 863, 866 (Ga. Ct. App. 1981) (emphasis in original)).

Courts grant summary judgment to insurers on bad faith claims where the issue of liability was close. See, e.g., [Homick v. Am. Casualty Co.](#), 433 S.E.2d 318, 319 (affirming grant of summary judgment to insurer on bad faith: “Ordinarily, the question of good or bad faith is for the jury, but when there is no evidence of unfounded reason for the nonpayment, or if the issue of liability is close, the court should disallow imposition of bad faith penalties. Good faith is determined by the reasonableness of nonpayment of a claim.”) (quoting [Intl. Indem. Co. v. Collins](#), 367 S.E.2d 786, 786 (Ga. 1988)).

The Court finds that the issue of liability was close in this case. It was not “unreasonable” or “unfounded” for Defendant to deny coverage here and wait for this Court to determine the coverage required by the contract. As such, Defendant is entitled to summary judgment on Plaintiff's bad faith claim, and its Motion for Summary Judgment [Doc. No. 32] as to the bad faith claim is GRANTED.

### V. Conclusion

For the reasons stated above, Plaintiff's Motion to Exclude [Doc. No. 38] is GRANTED. Plaintiff's Motion for Judicial Notice [Doc. No. 39] is GRANTED in part and DENIED in part. As to coverage, Plaintiff's Motion for Partial Summary Judgment [Doc. No. 22] is GRANTED, and Defendant's Motion for Summary Judgment [Doc. No. 32] is DENIED as moot. As to the bad faith claim, Defendant's Motion for Summary Judgment [Doc. No. 32] is GRANTED. The Clerk is DIRECTED to enter judgment and close this action.

**SO ORDERED**, this 30th day of August, 2016.

### All Citations

Not Reported in F.Supp.3d, 2016 WL 4618761

“psychological tests” amount to medical examinations, and others do not. EEOC, *Enforcement Guidance: Disability—Related Inquiries and Medical Examinations of Employees*, at 5 (“psychological tests that are designed to identify a mental disorder or impairment” are medical exams, but “psychological tests that measure personality traits such as honesty, preferences, and habits” are not). No evidence shows that White Lake Ambulance insisted that Kroll’s psychological counseling involve one type of test or another. No evidence, indeed, shows that the ambulance service insisted she submit to *any* test while obtaining counseling. The majority acknowledges the same point. As it explains, a psychological-counseling requirement covers a range of treatments, some including “medical examinations,” some not. Maj. Op. at 816.

The breadth of services encompassed by a psychological-counseling requirement resolves this claim. For it means that *Kroll*, not the company, controlled her destiny—controlled in other words whether she sought counseling that included a medical examination or did not. No doubt, she might meet this requirement by seeing a psychologist or psychiatrist who used a medical examination. But, if so, that was her choice, not the company’s. If a trying boss insists that an employee arrive at work by eight o’clock the next morning, it is not the boss’s fault if the employee opts to meet the requirement by staying overnight in the office. So it is here. Kroll had the right to meet this counseling requirement on her own terms, some of which could lead to a medical examination and others of which would not. Because White Lake Ambulance did not “require” Kroll to obtain a “medical examination,” I must respectfully dissent.



**RETAIL VENTURES, INC.; DSW Inc.;  
DSW Shoe Warehouse, Inc., Plaintiffs—  
Appellees/Cross-Appellants,**

**v.**

**NATIONAL UNION FIRE INSURANCE  
COMPANY OF PITTSBURGH, PA.,  
Defendant-Appellant/Cross-Appellee.**

**Nos. 10–4576, 10–4608.**

United States Court of Appeals,  
Sixth Circuit.

Argued: July 17, 2012.

Decided and Filed: Aug. 23, 2012.

**Background:** Insured filed diversity action against insurer asserting claims for declaratory judgment, breach of computer fraud rider in commercial crime insurance policy, and breach of duty of good faith and fair dealing. Insurer counterclaimed seeking declaratory judgment in its favor. The United States District Court for the Southern District of Ohio, Michael H. Watson, J., granted summary judgment in part for both parties. Parties appealed.

**Holdings:** The Court of Appeals, Ralph B. Guy, Jr., Circuit Judge, held that:

- (1) on issue of first impression, phrase, “resulting directly from,” imposed traditional proximate cause standard;
- (2) “any loss” within meaning of proprietary information exclusion encompassed “theft” of data;
- (3) “proprietary information,” did not encompass stored data consisting of customer credit card and checking account information;
- (4) “Trade Secrets,” “proprietary information,” and “Confidential Processing Methods,” all pertained to secret information of insured involving manner in which business was operated;

- (5) insurer did not engage in bad faith by denying claim that had reasonable basis;
- (6) insurer's position was factually and legally reasonable; and
- (7) insurer did not engage in bad faith with regard to its investigation by requesting second opinion.

Affirmed.

#### 1. Insurance ⇨2098

Under Ohio law, an exclusion in an insurance policy will be interpreted to apply only to that which is clearly intended to be excluded.

#### 2. Insurance ⇨2090

Under Ohio law, the label given to a policy is not determinative of coverage.

#### 3. Insurance ⇨2140, 2153(1), 2165(1)

Phrase, "resulting directly from," in computer fraud rider of commercial crime insurance policy, imposed traditional proximate cause standard under Ohio law, as predicted by federal court, and, thus, computer hacker's infiltration of insured's computer system and insured's "direct" financial loss therefrom was covered under policy; coverage was not unambiguously limited to loss resulting "solely" or "immediately" from theft itself.

See publication Words and Phrases for other judicial constructions and definitions.

#### 4. Insurance ⇨1832(1)

Under Ohio law, a policy prepared by an insurer must be construed liberally in favor of the insured and strictly against the insurer if the language used is doubtful, uncertain, or ambiguous.

#### 5. Insurance ⇨2140, 2153(1)

Plain and ordinary meaning of "any loss" within meaning of proprietary information exclusion in computer fraud rider of commercial crime insurance policy under Ohio law encompassed "theft" of data, or fraudulent accessing and copying of in-

formation, on insured's computer system, even if it was not removed, destroyed, or rendered inaccessible in the process.

See publication Words and Phrases for other judicial constructions and definitions.

#### 6. Insurance ⇨2098, 2116

There is a general presumption under Ohio law that what is not clearly excluded from coverage is included; that is, an exclusion from liability must be clear and exact in order to be given effect.

#### 7. Insurance ⇨1835(2), 1836, 2098

If an exclusion is ambiguous under Ohio law, it is construed in favor of affording coverage to the insured.

#### 8. Insurance ⇨2117

Under Ohio law, the insurer bears the burden of proving the applicability of an exclusion in its policy.

#### 9. Insurance ⇨2140

"Proprietary information," within meaning of exclusion in computer fraud rider of commercial crime insurance policy under Ohio law, did not encompass stored data consisting of customer credit card and checking account information, since that information was owned or held by many, including customer, financial institution, and merchants to whom information was provided in ordinary stream of commerce; loss of proprietary information would mean loss of information to which insured owned or held single or sole right.

See publication Words and Phrases for other judicial constructions and definitions.

#### 10. Insurance ⇨2140

"Stolen" customer information that had been obtained from customers in order to receive payment was not encompassed within "proprietary information," "Trade Secrets," and "Confidential Processing Methods," in exclusion in computer fraud

rider of commercial crime insurance policy, since all those terms pertained to secret information of insured involving manner in which business was operated; “other confidential information of any kind” had to be interpreted as part of sequence because broad application would have swallowed not only other terms but also coverage for computer fraud.

#### 11. Statutes ⇨194

Under the principle of ejusdem generis, the general term must take its meaning from the specific terms with which it appears.

#### 12. Contracts ⇨156

##### Insurance ⇨1805

The principle of ejusdem generis, i.e., the general term must take its meaning from the specific terms with which it appears, may be used when interpreting insurance and other contracts under Ohio law.

#### 13. Insurance ⇨3360

Insurer did not engage in bad faith under Ohio law with regard to its denial of claim for coverage under computer fraud rider in commercial crime insurance policy even though reasonable basis existed for insured’s claim; to incorporate default-ambiguity rule of construction to mean that insurer could deny coverage in good faith only if it had reason to believe that its interpretation was only reasonable one would have conflated two claims and equated bad faith with breach of contract.

#### 14. Insurance ⇨3336

Under Ohio law, an insurer fails to exercise good faith when it refuses to pay a claim without reasonable justification; denial of a claim may be reasonably justified when the claim was fairly debatable and the refusal was premised on either the

status of the law at the time of the denial or the facts that gave rise to the claim.

#### 15. Insurance ⇨3360

Insurer’s position in denying claim for coverage under computer fraud rider in commercial crime insurance policy, that consumer information fell within plain and ordinary meaning of “other confidential information of any kind,” though unsuccessful, was factually and legally reasonable, in light of confidential nature of the customer information and position that ejusdem generis did not apply, and thus denial was not in bad faith under Ohio law.

#### 16. Insurance ⇨3361

Insurer did not engage in bad faith under Ohio law with regard to its investigation of claim for coverage under computer fraud rider in commercial crime insurance policy by requesting second opinion; request for second opinion did not make investigation one-sided.

---

**ARGUED:** Steven G. Janik, Janik L.L.P., Cleveland, Ohio, for Appellant/Cross-Appellee. James E. Arnold, James E. Arnold & Associates, LPA, Columbus, Ohio, for Appellees/Cross-Appellants. **ON BRIEF:** Steven G. Janik, Thomas D. Lambros, Crystal L. Maluchnik, Janik L.L.P., Cleveland, Ohio, for Appellant/Cross-Appellee. James E. Arnold, Gerhardt A. Gosnell II, James E. Arnold & Associates, LPA, Columbus, Ohio, Joshua Gold, Anderson Kill & Olick, P.C., New York, New York, for Appellees/Cross-Appellants.

Before: GUY, and CLAY, Circuit Judges; HOOD, District Judge.\*

\*The Honorable Denise Page Hood, United States District Judge for the Eastern District

of Michigan, sitting by designation.

## OPINION

RALPH B. GUY, JR., Circuit Judge.

Defendant National Union Fire Insurance Company of Pittsburgh, PA, a subsidiary of AIG, Inc., appeals from the final judgment entered in favor of plaintiffs Retail Ventures, Inc., DSW Inc., and DSW Shoe Warehouse, Inc., for more than \$6.8 million in stipulated losses and prejudgment interest. Plaintiffs prevailed on cross-motions for summary judgment with respect to the claim for coverage under a computer fraud rider to a “Blanket Crime Policy” for losses resulting from a computer hacking scheme that compromised customer credit card and checking account information. Defendant claims the district court erred: (1) in finding that plaintiffs suffered a loss “resulting directly from” the “theft of any Insured property by Computer Fraud”; and (2) in rejecting application of the exclusion of “any loss of proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind.” Plaintiffs’ cross-appeal challenges the district court’s rejection of the tort claim for breach of the duty of good faith and fair dealing. After review of the record and consideration of the arguments presented on appeal, the judgment of the district court is affirmed.

## I.

The circumstances surrounding the hacking incident are not at issue on appeal, although it is now known that it was part of a larger scheme led by convicted computer hacker Albert Gonzalez. Briefly, between February 1 and February 14, 2005, hackers used the local wireless network at one DSW store to make unauthorized access to plaintiffs’ main computer system and download credit card and checking

account information pertaining to more than 1.4 million customers of 108 stores.<sup>1</sup> Fraudulent transactions followed using the stolen customer payment information, to which plaintiffs were first alerted by one of the affected credit card companies on March 2, 2005. Plaintiffs launched an investigation that quickly revealed the data breach; National Union was notified of the insurance claim at issue; and, in April 2005, National Union, through its affiliate AIG Technical Services, Inc., advised plaintiffs that an investigation would be carried out “under a full reservation of all rights and defenses at law, in equity, and under the terms and conditions of the bond.”

In the wake of the data breach, plaintiffs incurred expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with investigations by seven state Attorney Generals and the Federal Trade Commission (FTC). The FTC’s inquiry was resolved administratively with a consent decree requiring, *inter alia*, that plaintiffs establish and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. *In the Matter of DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006). The largest share of the losses—more than \$4 million—arose from the compromised credit card information: namely, costs associated with charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard. That amount was determined by the settlement of plaintiffs’ contractual obligations with credit card processor, National Processing Com-

1. Information from the magnetic stripe on the back of customer credit cards and customer bank account and driver’s license information

was received and stored electronically on plaintiffs’ computer system.

pany, LLC (a/k/a BA Merchant Services, LLC).

Plaintiffs submitted an initial partial proof of loss and supporting information in September 2005. Defendant sent that partial claim to outside counsel for analysis of the coverage question—first to John Petro, Esq., and then to Thomas Hanlon, Esq.—before denying coverage for the reasons stated in a letter dated January 30, 2006. Petro initially opined that there was coverage under the computer fraud rider, but he later backtracked and agreed with Hanlon’s assessment that the loss was excluded. Asserting that defendant’s investigation was so inadequate or “one-sided” as to establish bad faith, plaintiffs point to defendant’s pursuit of the second opinion from an attorney whose firm regularly provided services to AIG and Petro’s explanation of how he “missed” the exclusion pointed out by Hanlon.

The January 2006 denial letter questioned the “location” of the loss; stated that the loss appeared to be excluded because it related to the theft of confidential customer information excluded by Paragraph 9 of the computer fraud rider; and added in a footnote that the policy did not cover “indirect loss” in light of Exclusion 2(m). Plaintiffs responded by disclosing additional information—including the forensic analysis of the computer breach prepared a year earlier—to defendant on April 24, 2006; submitting a supplemental partial proof of loss on May 8, 2006; and commencing this lawsuit on May 9, 2006. Defendant subsequently clarified its position, but continued to deny coverage in a letter dated May 12, 2006. That letter explained that coverage would still be excluded because the claims arose from

“third party theft of proprietary confidential customer credit card information.” A final proof of loss was not submitted by plaintiffs until June 29, 2007.

Plaintiffs’ claims for declaratory judgment, breach of contract, and breach of the duty of good faith and fair dealing were answered by defendant’s counterclaim seeking declaratory judgment in its favor. Defendant alleged that plaintiffs had not sustained loss “resulting directly from” the theft of customer information; that general exclusions in Paragraph 2(k), (m) and (n) applied; and that coverage was specifically excluded under Paragraph 9 of Endorsement 17. After discovery, cross-motions for summary judgment were filed in two waves. The district court resolved the coverage and exclusion issues in plaintiffs’ favor in the opinion and order issued March 30, 2009, and rejected plaintiffs’ claims of bad faith in a separate opinion and order issued September 28, 2010. Then, to resolve the issues that remained for trial without waiving the right to appeal, the parties stipulated to a summary of losses incurred by plaintiffs (minus the self-insured retention) totaling more than \$5.3 million and the calculation of associated prejudgment interest in excess of \$1.49 million. Judgment was entered accordingly. Defendant appealed, and plaintiffs have cross-appealed.<sup>2</sup>

## II.

Summary judgment is appropriate when, viewing the factual inferences and all reasonable inferences in favor of the nonmoving party, there are no genuine issues of material fact in dispute and the moving party is entitled to judgment as a

2. Defendant filed a motion to strike a large part of plaintiffs’ fourth brief on the grounds that it improperly addressed the coverage and exclusion issues that were raised in defendant’s appeal. Because plaintiffs’ fourth brief

permissibly addressed the related issues of its cross-appeal challenging the finding that defendant was reasonably justified in denying coverage, the motion to strike is DENIED.

matter of law. *See* FED.R.CIV.P. 56(a). Our review of the district court's decision granting summary judgment is *de novo*. *La Quinta Corp. v. Heartland Props. LLC*, 603 F.3d 327, 335 (6th Cir.2010). We apply the same standard in reviewing decisions on cross-motions for summary judgment, evaluating each motion on its own merits. *Id.*

### A. Defendant's Appeal

In this diversity action governed by Ohio law, contract interpretation is a question of law for the court. *Leber v. Smith*, 70 Ohio St.3d 548, 639 N.E.2d 1159, 1163 (1994). The district court correctly summarized the general principles of contract interpretation as follows:

In interpreting an insurance contract, the court is to give effect to the intent of the parties to the agreement. *Hamilton Ins. Serv., Inc. v. Nationwide Ins. Cos.*, 86 Ohio St.3d 270, 273 [714 N.E.2d 898] (1999), citing *Employers' Liab. Assur. Corp. v. Roehm*, 99 Ohio St. 343 [124 N.E. 223] (1919) (syllabus). Ohio courts shall give insurance contract terms their plain and ordinary meaning unless another meaning is clearly apparent from the contents of the policy. *Alexander v. Buckeye Pipe Line Co.*, 53 Ohio St.2d 241 [374 N.E.2d 146] (1978) (syllabus ¶ 2). Further, a court must give meaning to every paragraph, clause, phrase, and word. *Affiliated FM Ins. Co. v. Owens-Corning Fiberglas Corp.*, 16 F.3d 684, 686 (6th Cir.1994). When the language of a written contract is clear, a court may look no further than the writing itself to find the intent of the parties. *Id.* As a matter of law, a contract is unambiguous if it can be given a definite legal meaning. *Westfield Ins. Co. v. Galatis*, 100 Ohio St.3d 216, 219 [797 N.E.2d 1256] (2003), citing *Gulf Ins. Co. v. Burns Motors, Inc.*, 22 S.W.3d 417, 423 (Tex.2000).

A term is ambiguous if it is reasonably susceptible of more than one meaning. *St. Mary's [Marys] Foundry, Inc. v. Employers Ins. of Wausau*, 332 F.3d 989, 992 (6th Cir.2003) (citations omitted). Where the written contract is standardized and between parties of unequal bargaining power, an ambiguity in the writing will be interpreted strictly against the drafter and in favor of the nondrafting party. *Cent. Realty Co. v. Clutter*, 62 Ohio St.2d 411, 413 [406 N.E.2d 515] (1980). In the insurance context, as the insurer customarily drafts the contract, an ambiguity in an insurance contract is ordinarily interpreted against the insurer and in favor of the insured. *King v. Nationwide Ins. Co.*, 35 Ohio St.3d 208 [519 N.E.2d 1380] (1988) (syllabus). Nonetheless, this rule "will not be applied so as to provide an unreasonable interpretation of the words of the policy." *Morfoot v. Stake*, 174 Ohio St. 506 [190 N.E.2d 573] (1963) (syllabus ¶ 1).

We must determine how the Ohio courts would interpret the policy by looking first to Ohio law as determined by the Ohio Supreme Court, and then to all other sources. *Bovee v. Coopers & Lybrand CPA*, 272 F.3d 356, 361 (6th Cir.2001).

#### 1. Coverage

The only coverage provisions at issue are found in Endorsement 17's "Insuring Agreement XVIII," entitled "Computer & Funds Transfer Fraud Coverage." Specifically, defendant agreed in pertinent part to pay the insured for:

XVIII. Loss which the Insured shall sustain resulting directly from:

A. The theft of any Insured property by Computer Fraud; . . .

Endorsement 17 defines "Computer Fraud" to mean "the wrongful conversion of assets under the direct or indirect con-

trol of a Computer System by means of: (1) The fraudulent accessing of such Computer System; (2) The insertion of fraudulent data or instructions into such Computer System; or (3) The fraudulent alteration of data, programs, or routines in such Computer System.” As for “Insured property,” the policy generally defines the property interests covered as follows:

Section 5. The Insured property may be owned by the Insured, or held by the Insured in any capacity whether or not the Insured is liable for the loss thereof, or may be property as respects which the Insured is legally liable; provided, Insuring Agreements II, III and IV apply only to the interest of the Insured in such property, . . . .

Endorsement 17 adds that coverage applied “only with respect to . . . Money or Securities or Property located on the premises of the Insured.”

[1] Three general exclusions, which Endorsement 17 made applicable to Insuring Agreement XVIII, are relied upon by defendant to support the contention that only first party coverage was intended. Those exclusions, found in Section 2(k), (m), and (n) provide that the policy “does not apply”:

(k) to the defense of any legal proceeding brought against the Insured, or to fees, costs or expenses incurred or paid by the Insured in prosecuting or defending any legal proceeding whether or not such proceeding results or

would result in a loss to the Insured covered by this Policy, except as may be specifically stated to the contrary in this Policy;

. . . .

(m) to damages of any type for which the Insured is legally liable, except direct compensatory damages arising from a loss covered under this Policy;

(n) to costs, fees and other expenses incurred by the Insured in establishing the existence of or amount of loss covered under this Policy.

Except for (m), these exclusions represent limits placed on coverage for an insured’s own damages and do not speak to third party losses.<sup>3</sup>

Defendant does not dispute that the unauthorized access and copying of customer information stored on plaintiffs’ computer system involved the “theft of any Insured property by Computer Fraud,” (although there is no indication whether it was property owned by plaintiffs, held in some capacity by plaintiffs, or was property for which plaintiffs were legally liable). What is disputed, however, is whether the district court was correct in concluding in this case of first impression that the loss plaintiffs sustained was loss *resulting directly from* the theft of insured property by computer fraud. The district court predicted that the Ohio Supreme Court would follow those cases that interpret “resulting directly from” as imposing a traditional proximate cause standard in this context.

3. Defendant contends that the district court erred in rejecting its claim that attorney fees and costs incurred in responding to the FTC inquiry were specifically excluded by Section 2(k). Plaintiffs respond that its general liability insurer covered its defense costs for all “legal proceedings,” and that the claim in this case was limited to the attorney fees associated with the security breach itself and the FTC’s “nonpublic inquiry.” The term “legal proceeding” is not defined by the policy, but

FTC regulations distinguish “inquiries” and “investigations” from “formal adjudicative proceedings.” Compare 16 C.F.R. §§ 2.1, 2.4 and 2.8, with 16 C.F.R. §§ 3.1 and 3.2. An exclusion in an insurance policy will be interpreted to apply only to that which is clearly intended to be excluded. *Hybud Equip. Corp. v. Sphere Drake Ins. Co.*, 64 Ohio St.3d 657, 597 N.E.2d 1096, 1102 (1992). The district court did not err in this regard.



Accordingly, the district court concluded that “there is a sufficient link between the computer hacker’s infiltration of Plaintiffs’ computer system and Plaintiffs’ financial loss to require coverage under Endorsement 17.” Defendant argues that it was error to apply a proximate cause standard for several reasons.

**a. Fidelity Bond**

Defendant argues first that the commercial crime policy is a “fidelity bond” and therefore must be interpreted to provide only first party coverage. The district court found that the policy was “not a fidelity bond, *in toto*, as it provided more than fidelity coverage.” Further, the district court explained that Endorsement 17 “is not a fidelity bond as there is no mention of employee dishonesty” and that “the terms of Endorsement 17 indicate coverage for losses to third-party assets.” While it is true that “fidelity bonds,” or “financial institution bonds,” typically provide more than just fidelity coverage (*i.e.*, fidelity, forgery, on-premises and off-premises coverage), defendant overstates the significance of the analogy to the fidelity bond cases and the Standard Form 24, Standard Financial Institution Bond. See *First State Bank of Monticello v. Ohio Cas. Ins. Co.*, 555 F.3d 564, 568 (7th Cir. 2009) (Ill.law) (discussing fidelity bonds).

[2] Nonetheless, to the extent that the district court may have erroneously (or inconsistently) disregarded some fidelity bond cases on that basis, it is clear that the label given to a policy is not determinative of coverage. See *Hillyer v. State Farm Fire & Cas. Co.*, 97 Ohio St.3d 411, 780 N.E.2d 262, 265 (2002) (holding that “it is the type of coverage provided, not the label affixed by the insurer, that determines the type of policy”). Moreover, even in the context of fidelity or dishonest employee coverage, there is no universal agreement among the courts concerning

the meaning of the phrase “resulting directly from.” See *Universal Mortg. Corp. v. Wurttembergische Versicherung AG*, 651 F.3d 759, 762 (7th Cir.2011) (describing two competing “interpretive camps”); *The Question of Causation in Loan Loss Cases*, 11 FIDELITY L. ASS’N J. 97, 98 (2005) (noting “split” of authority).

**i. Direct–Means–Direct Approach**

Defendant urges this court to interpret the “resulting directly from” language as unambiguously requiring that the theft of property by computer fraud be the “sole” and “immediate” cause of the insured’s loss. See, *e.g.*, *RBC Mortg. Co. v. Nat’l Union Fire Ins. Co. of Pittsburgh*, 349 Ill.App.3d 706, 285 Ill.Dec. 908, 812 N.E.2d 728 (2004) (Ill.law) (adopting a direct-means-direct standard). Under this approach, loss “resulting directly from” employee misconduct refers only to the insured’s *own* loss from employee misconduct and not the insured’s vicarious liability to third parties. See *Vons Cos. v. Fed. Ins. Co.*, 212 F.3d 489, 492–93 (9th Cir. 2000) (direct means no vicarious liability); *Aetna Cas. & Sur. Co. v. Kidder, Peabody & Co.*, 246 A.D.2d 202, 209–10, 676 N.Y.S.2d 559 (1998) (finding no coverage for third-party claims arising out of misconduct of employee who disclosed confidential information to others that resulted in massive insider trading losses). The Seventh Circuit describes this line of authority as holding that “when an insured incurs liability to a third party—whether in contract or tort—as a result of employee misconduct, financial loss resulting from that liability is not ‘directly’ caused by the employee misconduct and therefore is not covered by fidelity bonds containing direct-loss language.” *Universal Mortg.*, 651 F.3d at 762 (discussing *RBC* (Ill.law) and *Tri City Nat’l Bank v. Fed. Ins. Co.*, 268 Wis.2d 785, 674 N.W.2d 617, 622–24 (App.2003) (Wis.law)).

Courts that have adopted the direct-means-direct approach generally emphasize the historical context of fidelity bonds, which typically bundle indemnity coverage for specific risks, as well as the specific modification to Standard Form 24, Financial Institution Bond, that adopted the loss “resulting directly from” language with the purported intention of narrowing coverage. *See id.* at 761–62; *Monticello*, 555 F.3d at 570 (discussing revisions to standard form). These decisions also reason that “resulting directly from” suggests stricter causation than proximate cause because “directly” implies an immediacy to the fraud. *See RBC*, 285 Ill.Dec. 908, 812 N.E.2d at 736–37 (rejecting proximate cause as “too broad to capture accurately the intent behind the phrase ‘loss resulting directly from’”). In *Universal Mortgage*, the Seventh Circuit also relied on the fact that the state courts in Wisconsin had already adopted the direct-means-direct approach in *Tri City*. 651 F.3d at 762; *see also Direct Mortg. Corp. v. Nat’l Union Fire Ins. Co. of Pittsburgh*, 625 F.Supp.2d 1171, 1176 (D.Utah 2008) (concluding that the Utah Supreme Court would most likely adopt the direct-means-direct approach as better reasoned and more consistent with the traditional nature of fidelity bonds and the specific language at issue).<sup>4</sup>

## ii. *Flagstar Bank*

Defendant argues next that this court has already adopted a “heightened” standard for demonstrating “loss resulting directly from” forgery under a fidelity bond.

*Flagstar Bank, FSB v. Fed. Ins. Co.*, 260 Fed.Appx. 820 (6th Cir.2008) (Mich.law) (unpublished); *see also Merchants Bank & Trust v. Cincinnati Ins. Co.*, No. 06–cv–561, 2008 WL 728332, at \*4 (S.D.Ohio Mar. 14, 2006) (unpublished). However, this argument overstates both the holding in *Flagstar* and its application to this case.

First, there was no issue of liability to third parties in *Flagstar* as the insured was seeking coverage for its own losses incurred when a mortgage broker defaulted on a \$20 million line of credit obtained using fraudulent mortgage documents that were premised on *fictitious* collateral. *Flagstar*, 260 Fed.Appx. at 821. This court held that because the forged promissory notes “would not have held value even if they had authentic signatures,” *Flagstar*’s loss did *not* result directly from the forgery. *Id.* at 822–23. We explained that: “The district court correctly followed the logic of cases holding that financial institution bonds, which cover losses resulting either directly or indirectly from forgery, do not cover losses arising from the extension of loans based on fictitious collateral.” *Id.* at 823 (citations omitted); *see also Beach Comm. Bank v. St. Paul Mercury Ins. Co.*, 635 F.3d 1190, 1196 (11th Cir.2011). This was also the basis for distinguishing this court’s prior decision in *Union Planters Bank*, which involved forged signatures on duplicate mortgages. *See Union Planters Bank, NA v. Cont’l Cas. Co.*, 478 F.3d 759 (6th Cir.2007).

4. Even these cases, however, recognize that “there are instances when third party losses may be covered under fidelity bonds.” *Tri City*, 674 N.W.2d at 626, n. 9. A direct loss may be caused by an “employee’s theft of property for which it is legally liable, the typical case being where the insured is a bailee or trustee of property.” *Vons*, 212 F.3d at 491; *see also First Defiance Fin. Corp. v. Progressive Cas. Ins. Co.*, 688 F.Supp.2d

703, 707 (N.D.Ohio 2010) (holding that employer incurred direct loss resulting from the theft of customer funds held in trust by the employer under fidelity bond), *aff’d in part*, 688 F.3d 265 (6th Cir.2012). We do not reach plaintiffs’ alternative argument that even under a direct-means-direct approach the losses would not be excluded because this case involves “theft” of insured property from plaintiffs’ computer system.

Further, *Flagstar's* reference to a "heightened" causation standard arose in distinguishing *First National Bank of Manitowoc v. Cincinnati Insurance Co.*, 485 F.3d 971, 979 (7th Cir.2007), which held that loss involving fictitious collateral could be covered as loss "by reason of" the forgery under Insuring Agreement E (even if it would not be covered as a loss "resulting directly from" forgery under Insuring Agreement D). This court also distinguished dicta from *Manitowoc* that criticized a decision of the Georgia Court of Appeals for failing to address the separate language of Insuring Agreements D and E. *Flagstar*, 260 Fed.Appx. at 824 n. 1. Despite this court's implicit acceptance of the distinction drawn in *Manitowoc*, it overstates the case to say *Flagstar* adopted a heightened causation standard for the phrase "resulting directly from" in a financial institution bond or commercial crime policy. Cf. *Union Planters*, 478 F.3d at 764 (applying Tennessee's proximate cause standard to determine whether loss "resulted directly from" loans extended on the basis of forged collateral).

### iii. Proximate Cause

Plaintiffs maintain that the district court correctly concluded that the Ohio Supreme Court would follow those courts that have adopted proximate cause as the standard for determining "direct loss" in the fidelity coverage context. See, e.g., *Auto Lenders Acceptance Corp. v. Gentilini Ford, Inc.*, 181 N.J. 245, 854 A.2d 378, 385–86 (2004) (N.J.law); *Frontline Processing Corp. v. Am. Econ. Ins. Co.*, 335 Mont. 192, 149 P.3d 906, 909–11 (2006); *Scirex Corp. v. Fed. Ins. Co.*, 313 F.3d 841, 850 (3d Cir. 2002) (Pa.law); *FDIC v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 205 F.3d 66, 76 (2d Cir.2000) (N.J.law); *Resolution Trust Corp. v. Fid. & Deposit Co. of Md.*, 205 F.3d 615, 655 (3d Cir.2000) (N.J.law); *Jefferson Bank v. Progressive Cas. Ins. Co.*,

965 F.2d 1274, 1281–82 (3d Cir.1992) (Pa.law).

In *Auto Lenders*, the most prominently cited of these cases, the insurer argued that losses incurred by the insured in repurchasing fraudulent installment loan contracts were not covered because there was no "direct loss of or damage to" property, money, or securities as a result of employee dishonesty. Rejecting this contention, the New Jersey Supreme Court adopted "the conventional proximate cause test as the correct standard to apply when determining whether a loss resulted from the dishonest acts of an employee." *Auto Lenders*, 854 A.2d at 387. The Court explained (1) that although the New Jersey courts had not decided the issue in the context of fidelity or dishonest employee coverage, proximate cause had been applied in determining direct loss under other kinds of insurance; (2) that federal courts, including the Second and Third Circuits in *Scirex*, *FDIC*, and *Resolution Trust*, had adopted a proximate cause standard for determining "direct loss" as a result of employee dishonesty; and (3) that this standard was consistent with the general principle of New Jersey law that coverage provisions are to be interpreted broadly.

Similarly, the Montana Supreme Court held that "the term 'direct loss' when used in the context of employee dishonesty coverage afforded under a business owner's liability policy, applies to consequential damages incurred by the insured that were proximately caused by the alleged dishonesty." *Frontline Processing*, 149 P.3d at 911. After its CFO embezzled funds and failed to pay its payroll and income taxes, Frontline sought coverage for costs it incurred to investigate its employee's misconduct, address the financial condition of the company, and pay costs, fees, penalties and interest assessed by the IRS. The

Court distinguished *Tri City, RBC*, and *Vons* because they involved third party claims; concluded that—as in *Jefferson, Scirea*, and *Auto Lenders*—“a proximate cause analysis [was] appropriate in determining whether a loss is ‘direct’ under a fidelity insurance policy”; and added that this comported with the general application of proximate cause to losses under other kinds of insurance policies under state law. *Id.* at 911.

### b. Analysis

[3,4] Without ignoring that this is a commercial crime policy directed at the insured’s loss and not a commercial liability policy, our task is to determine the intention of the parties from the plain and ordinary meaning of the specific language used. A policy prepared by an insurer “must be construed liberally in favor of the insured and strictly against the insurer if the language used is doubtful, uncertain or ambiguous.” *Am. Fin. Corp. v. Fireman’s Fund Ins. Co.*, 15 Ohio St.2d 171, 239 N.E.2d 33, 35 (1968). Despite defendant’s arguments to the contrary, we find that the phrase “resulting directly from” does not unambiguously limit coverage to loss resulting “solely” or “immediately” from the theft itself. In fact, Endorsement 17 provided coverage for loss that the insured sustained “resulting directly from” the “theft of any Insured property by Computer Fraud,” which includes the “wrongful conversion of assets under the direct or indirect control of a Computer System by means of . . . fraudulent accessing of such Computer System.” Nor are we persuaded that the general exclusions in Section 2(k), (m), and (n) clarify the scope of the computer fraud coverage under Endorsement 17. When the exclusionary language is taken with the computer fraud coverage provisions in Endorsement 17, the meaning of the phrase “resulting directly from” is still ambiguous.

The Ohio courts have not decided whether to apply proximate cause in the context of a fidelity bond or commercial crime policy. Despite plaintiffs’ suggestion otherwise, no implicit holding on the issue of causation can be read into the one Ohio court decision that involved a claim for loss “resulting directly from” forgery under a financial institution bond. *See Bank One, Steubenville, NA v. Buckeye Union Ins. Co.*, 114 Ohio App.3d 248, 683 N.E.2d 50 (1996) (holding that use of a signature stamp without authorization constituted forgery), *appeal not allowed*, 77 Ohio St.3d 1548, 674 N.E.2d 1186 (Ohio Jan. 29, 1997). Nonetheless, plaintiffs have identified a few Ohio court decisions in which the court applied a proximate cause standard to determine whether there was a “direct loss” under other kinds of first party coverage. *See, e.g., Amstutz Hatcheries of Celina, Inc. v. Grain Dealers Mut. Ins. Co.*, No. 4–77–4, 1978 WL 215799, at \*1–2 (Ohio App. Mar. 15, 1978) (finding coverage against loss of chickens “directly and immediately resulting from” lightning included suffocation when lightning knocked out power to ventilation system); *Yunker v. Republic–Franklin Ins. Co.*, 2 Ohio App.3d 339, 442 N.E.2d 108, 113–14 (1982) (applying proximate cause standard to determine “direct loss” under windstorm policy). Defendant argues that these cases are distinguishable, but has not identified any Ohio decisions that decline to apply a proximate cause standard in determining “direct” loss. Although not relied upon by the district court, these cases support the conclusion that the Ohio courts would apply a proximate cause standard to determine whether the loss was covered in this case.

Consistent with general principles of insurance contract interpretation under Ohio law, we agree with the district court’s determination that the Ohio Supreme Court would apply a proximate cause standard to determine whether plaintiffs sustained loss

“resulting directly from” the “theft of Insured property by Computer Fraud.”

## 2. Exclusion 9

[5–8] There is a general presumption under Ohio law that what is not clearly excluded from coverage is included. *Moorman v. Prudential Ins. Co. of Am.*, 4 Ohio St.3d 20, 445 N.E.2d 1122, 1124 (1983). That is, “an exclusion from liability must be clear and exact in order to be given effect.” *Lane v. Grange Mut. Cos.*, 45 Ohio St.3d 63, 543 N.E.2d 488, 490 (1989). If an exclusion is ambiguous, it is construed in favor of affording coverage to the insured. *St. Marys Foundry, Inc. v. Emp’rs Ins. of Wausau*, 332 F.3d 989, 993 (6th Cir.2003) (Ohio law). The insurer bears the burden of proving the applicability of an exclusion in its policy. *Cont’l Ins. Co. v. Louis Marx Co.*, 64 Ohio St.2d 399, 415 N.E.2d 315, 317 (1980).

Apart from the question of coverage, defendant relied on the following specific exclusion in Paragraph 9 of Endorsement 17:

9. Coverage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind.

Defendant argues that the district court erred in finding that this exclusion did not bar coverage in this case.

Relying on dictionary definitions for the word “loss,” the district court found that “loss of” was ambiguous because it could reasonably mean either “destruction of” or “deprivation/losing possession of” the specified items. However, as defendant argues, the existence of more than one dictionary definition does not make a term ambiguous. See *AGK Holdings, Inc. v. Essex Ins. Co.*, 142 Fed.Appx. 889, 892 (6th Cir.2005) (unpublished). By excluding coverage for *any* loss, Paragraph 9 plainly excludes coverage for both loss by

destruction and loss of possession of the specified items. Plaintiffs also argue that “any loss” should not be read to include fraudulent accessing and copying of information without removing, interfering with access, or destroying the data on plaintiffs’ computer system. However, the plain and ordinary meaning of “any loss” encompasses the “theft” of such data even if it is not destroyed or rendered inaccessible in the process. Finally, the district court found that the exclusion did not clearly include financial loss because “any loss of” an item is not the same as *financial loss attributed to* the loss of an item. However, if there were no coverage for the loss of the information itself, there would also be no coverage for damages resulting from the loss of the information.

[9] Nonetheless, the district court also concluded that even if the copying of customer information was a “loss” it was not a loss of “proprietary information . . . or other confidential information of any kind.” Defendant has not shown that this was error. Defendant argues first that plaintiffs should be bound to an interpretation consistent with the assertions made by counsel in five short cover letters to the FTC stating that plaintiffs considered “the enclosed documents to be highly confidential, as the documents address security measures used by DSW to maintain the confidentiality of its trade secret and proprietary information (which includes customer information).” On the contrary, the parenthetical reference to “customer information” cannot be considered an admission regarding the applicability of the Exclusion in paragraph 9. Moreover, plaintiffs respond that the documents which were disclosed under these cover letters did not actually include the downloaded customer payment information in question.

Examining the exclusion for its plain and ordinary meaning, the district court

concluded that loss of proprietary information would mean the loss of information “to which Plaintiffs own or hold single or sole right.” In fact, as the district court found, the stolen customer information was not “proprietary information” at all, since the information is owned or held by many, including the customer, the financial institution, and the merchants to whom the information is provided in the ordinary stream of commerce. The district court did not err in finding that the stored data consisting of customer credit card and checking account information would not come within the plain and ordinary meaning of “proprietary information.”<sup>5</sup>

[10] Defendant made no claim that the customer information constituted “Trade Secrets” or “Confidential Processing Methods,” but argued that the customer information came within the broad “catch-all” clause excluding coverage for “loss of . . . confidential information of any kind.” As defendant argued, the evidence shows that plaintiffs recognized in contracts with credit card companies, under standards applicable to the processing of credit card payments, and in internal policies and procedures, that the confidentiality of customer credit card and checking account information would and should be protected from unauthorized access or disclosure. However, to interpret “other confidential information of any kind” as defendant urges—to mean any information belonging to anyone that is expected to be protected from unauthorized disclosure—would swallow not only the other terms in this exclusion but also the coverage for computer fraud.

5. Defendant cites to a partially reversed decision that described extensive and detailed customer profiles (including personal information, preferences, and travel histories) kept by the Four Seasons Hotels as proprietary in a case alleging misappropriation of trade secrets and violation of federal statutes. See

[11, 12] The district court rejected the broad interpretation of “confidential information” urged by defendant because, under the principle of *ejusdem generis*, the general term must take its meaning from the specific terms with which it appears. See *Allinder v. Inter-City Prods. Corp.*, 152 F.3d 544, 549 (6th Cir.1998). Although defendant argues that this rule of statutory construction does not apply to insurance contracts, the Ohio courts have used the doctrine of *ejusdem generis* in interpreting insurance and other contracts. See, e.g., *Sherwin-Williams Co. v. Travelers Cas. & Sur. Co.*, No. 82867, 2003 WL 22671621, at \*4 (Ohio App. Nov. 13, 2003) (applying doctrine to limit “invasion of right to private occupancy” to preceding terms “wrongful entry” and “eviction”); *Direct Carpet Mills Outlet v. Amalg. Realty Co.*, No. 87AP-101, 1988 WL 84405, at \*3 (Ohio App. Aug. 11, 1988) (finding “accident of any kind” in exclusion must be read to refer to accidents similar in kind to the terms “fire, explosion, and wind” that preceded it). Moreover, defendant’s contention that the doctrine does not apply because the exclusion does not list specific terms followed by a general term is without merit. The terms “Trade Secrets” and “Confidential Processing Methods” were capitalized, suggesting a specific meaning, although they were not defined in the policy.

Looking to the common law definition of “trade secrets,” and dictionary definitions for “confidential” “processing” and “method,” the district court reasonably concluded that the term “Trade Secrets” means “Plaintiffs’ information which is used in

*Four Seasons Hotels & Resorts BV v. Consorcio Barr, SA.*, 267 F.Supp.2d 1268, 1276–78 (S.D.Fla.2003), *rev’d in part without opinion*, 138 Fed.Appx. 297 (11th Cir.2005). There is no indication that plaintiffs’ centrally stored file of customer payment data contained similarly proprietary information.

*Plaintiffs'* business, and which gives *Plaintiff* an opportunity to obtain advantage over competitors who do not know or use the information." Similarly, "Confidential Processing Methods" means *plaintiffs'* secret process or technique for doing something, "which in the context of the Exclusion, relates to Plaintiff[s'] business operation." The district court did not err in finding that "proprietary information," "Trade Secrets," and "Confidential Processing Methods," are specific terms that all pertain to secret information of plaintiffs involving the manner in which the business is operated. The last item, "other confidential information of any kind," is most certainly general and should be interpreted as part of the sequence to refer to "other secret information of *Plaintiffs* which involves the manner in which the business is operated." The "stolen" customer information was not plaintiffs' confidential information, but was obtained from customers in order to receive payment, and did not involve the manner in which the business is operated. The district court did not err in finding that the loss in this case was not clearly excluded by Paragraph 9 of Endorsement 17.

#### B. Plaintiffs' Cross-Appeal

[13, 14] Plaintiffs appeal the decision granting summary judgment to defendant on the tort claim for breach of the duty of good faith and fair dealing under Ohio law. See *Hoskins v. Aetna Life Ins. Co.*, 6 Ohio St.3d 272, 452 N.E.2d 1315, 1316 (1983). An insurer fails to exercise good faith when it refuses to pay a claim without "reasonable justification." *Zoppo v. Homestead Ins. Co.*, 71 Ohio St.3d 552, 644 N.E.2d 397, 399-400 (1994) (holding that actual intent is not an element of the tort of bad faith); see also *Corbo Props., Ltd. v. Seneca Ins. Co.*, 771 F.Supp.2d 877, 880

(N.D. Ohio 2011). Denial of a claim may be reasonably justified when "the claim was fairly debatable and the refusal was premised on either the status of the law at the time of the denial or the facts that gave rise to the claim." *Tokles & Son, Inc. v. Midwestern Indemn. Co.*, 65 Ohio St.3d 621, 605 N.E.2d 936, 943 (1992).

First, arguing that the district court applied the wrong legal standard, plaintiffs contend that Ohio's default-ambiguity rule of construction means that an insurer can deny coverage in good faith *only if* it had reason to believe that its interpretation was the *only reasonable one*. There is no support for this proposition in Ohio law, which recognizes distinct standards for determining breach of contract and breach of the duty of good faith. In fact, the Ohio Supreme Court has stated that "[m]ere refusal to pay insurance is not, in itself, conclusive of bad faith." *Hoskins*, 452 N.E.2d at 1320; see *Schuetz v. State Farm Fire & Cas. Co.*, 147 Ohio Misc.2d 22, 890 N.E.2d 374, 393-94 (Ohio Ct.Com.Pl.2007) (rejecting argument that breach of the duty to defend also establishes bad faith). To incorporate the default-ambiguity canon into a bad faith claim as plaintiffs suggest would conflate the two claims and equate bad faith with breach of contract.<sup>6</sup>

[15] Next, plaintiffs challenge the district court's conclusion that the coverage question was "fairly debatable" on the grounds that the defendant did not, in fact, rely on the "direct loss" issue in denying coverage. Although the denial letters did not specifically reference the "resulting directly from" language, there was mention of the fact that the policy did not cover "indirect losses" such as fines, penalties and interest. Further, as the district court concluded, the failure to reference

6. Plaintiffs' reliance on the Tenth Circuit's decision to the contrary in *Wolf v. Prudential*

*Insurance Co. of America*, 50 F.3d 793, 800 (10th Cir.1995), is misplaced.

the “resulting directly from” language in the claim file itself does not demonstrate bad faith on the part of the insurer.

Moreover, the district court also concluded that defendant had reasonable justification for the refusal to pay because its interpretation of the Exclusion in paragraph 9 was incorrect but not unreasonable. Plaintiffs disagree and again argue that defendant did not have an objectively reasonable basis to believe that its interpretation of the exclusion was the *only* reasonable one. On the contrary, as the district court found, defendant’s claim that the consumer information fell within the plain and ordinary meaning of “other confidential information of any kind” was factually and legally reasonable in light of the confidential nature of the customer information and the claim that *ejusdem generis* did not apply.

[16] Nor is there a question about the adequacy or reasonableness of defendant’s investigation of the claim. In truth, plaintiffs’ complaint is not really that the investigation was inadequate, but rather that defendant was not satisfied with the first legal opinion it received. We cannot conclude, however, that requesting a second opinion under the circumstances made the investigation so one-sided as to constitute bad faith.

**AFFIRMED.**



**Bret A. LEWIS and Rebecca J. Lewis,**  
**Plaintiffs–Appellees,**

**v.**

**UNITED JOINT VENTURE,**  
**Defendant–Appellant.**

**No. 11–3044.**

United States Court of Appeals,  
Sixth Circuit.

Aug. 9, 2012.

**Background:** Creditors sought to enforce judgments they had obtained in Western District of Michigan. The United States District Court for the Northern District of Ohio, James S. Gwin, J., 2010 WL 4529956, entered orders of garnishment. Defendant appealed.

**Holdings:** The Court of Appeals, Clay, Circuit Judge, held that:

- (1) prior judgments could not be jointly setoff;
- (2) district court did not abuse its discretion by allowing subset of judgment creditors to collect full amount of attorney’s fees and costs that previously had been jointly awarded; and
- (3) creditors were required only to file certified copy of judgment with court in which enforcement was sought.

Affirmed.

## 1. Federal Courts ⇌813

A district court’s enforcement remedy issued pursuant to the Federal Rule of Civil Procedure governing execution is reviewed for abuse of discretion. Fed.Rules Civ.Proc.Rule 69, 28 U.S.C.A.

## 2. Federal Courts ⇌853

The Court of Appeals will reverse for an abuse of discretion where it is left with the definite and firm conviction that the



### **III.**

## **Data Breach Liability Policies**

Matthew T. Walsh, Esq. (Bar No. 208169)  
**CARROLL, McNULTY & KULL LLC**  
100 North Riverside Plaza, Suite 2100  
Chicago, Illinois 60606  
Telephone: (312) 800-5000  
Facsimile: (312) 800-5010  
Email: mwalsh@cmk.com

Attorneys for Plaintiff COLUMBIA CASUALTY COMPANY

**UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

COLUMBIA CASUALTY COMPANY	Case No.: 2:16-cv-3759
Plaintiff,	<b>COMPLAINT FOR DECLARATORY JUDGMENT, RESCISSION AND REIMBURSEMENT OF DEFENSE AND SETTLEMENT PAYMENTS</b>
v.	
COTTAGE HEALTH SYSTEM	
Defendant.	

Plaintiff COLUMBIA CASUALTY COMPANY (hereinafter "Columbia") by and through its attorneys, as and for Complaint against Defendant, hereby allege as follows:

**INTRODUCTION**

1. Pursuant to 28 U.S.C. § 2201, Columbia brings this action for Declaratory Judgment, Rescission and for Reimbursement of Defense and Settlement Payments made by Columbia on behalf of its insured.

2. This matter arises out of a data breach that resulted in the release of electronic private healthcare patient information stored on network servers owned, maintained and/or utilized by defendant COTTAGE HEALTH SYSTEM ("Cottage").

3. Cottage operates a network of hospitals located in Southern California, including Santa Barbara Cottage Hospital, Goleta Valley Cottage Hospital and Santa Ynez Valley Cottage Hospital (collectively, the "Hospitals.")

COMPLAINT FOR DECLARATORY JUDGMENT, RESCISSION AND REIMBURSEMENT

1           4.       Following the data breach, a class action lawsuit was commenced against  
2 Cottage in which the plaintiffs asserted claims against Cottage and others based on its alleged  
3 breach of California's Confidentiality of Medical Information Act ("CMIA"), California Civil  
4 Code §56, *et seq.* A settlement has been reached in the class action lawsuit for the amount of  
5 \$4.125 million.  
6

7           5.       Columbia incurred substantial defense costs and data breach response expenses  
8 on Cottage's behalf and funded the \$4.125 million class action settlement, subject to a  
9 complete reservation of rights.  
10

11           6.       The data breach is also the subject of an ongoing investigation conducted by the  
12 California Department of Justice regarding Cottage's potential violations of the federal Health  
13 Insurance Portability and Accountability Act ("HIPAA.")  
14

15           7.       Columbia issued a liability policy to Cottage providing claims made coverage  
16 for the October 1, 2013 to October 1, 2014 policy period.  
17

18           8.       Columbia seeks a declaration that it is not obligated to provide Cottage with a  
19 defense or indemnification in connection with any and all claims stemming from the data  
20 breach at issue.  
21

22           9.       Columbia also seeks a declaration that the liability policy issued to Cottage was  
23 issued in reliance upon material misrepresentations and/or omissions of fact and that,  
24 consequently, Columbia is entitled to rescind the policy as void *ab initio*.  
25

26           10.      Columbia also seeks a declaration of its entitlement to reimbursement in full  
27 from Cottage for any and all attorney's fees or related costs or expenses Columbia has paid or  
28 will pay in connection with the data breach and the defense and settlement of the class action  
lawsuit and any related proceedings and an award of damages consistent with such declaration.

**PARTIES, JURISDICTION AND VENUE**

11. Columbia is a corporation organized and existing under the laws of the State of Illinois and having its principal place of business located at CNA Plaza, Chicago, Illinois. Columbia is in the business of providing and underwriting insurance. Columbia is, and at all times relevant to this Complaint was, duly authorized to transact business in the State of California.

12. Upon information and belief, Cottage is a California organization with its principal place of business located at 400 West Pueblo Street, Santa Barbara, California 93105.

13. This litigation is a civil action over which this Court has original diversity jurisdiction pursuant to 28 U.S.C. §1332(a)(2) based on diversity of the parties and the amount in controversy.

14. The amount in controversy in this matter exceeds \$75,000. Columbia seeks a declaration that it is not obligated to provide coverage to Cottage for any portion of a \$4.125 million class action settlement, as well as additional potential regulatory liability, and seeks reimbursement of the settlement amount along with defense costs and data breach response expenses described more fully herein.

15. The insurance contract between Columbia and Cottage that is the subject of this declaratory judgment action was issued to Cottage in this District. Further, the alleged acts and omissions on the part of Cottage that precipitated the claims for which coverage is sought took place in this District. Therefore, venue is proper in this District pursuant to 28 U.S.C. § 1391.

**FACTUAL BACKGROUND**

**A. The Underlying Action**

16. On or about January 27, 2014, a proposed class action was commenced in California Superior Court, Orange County styled Kenneth Rice, et al. v. INSYNC, Cottage Health System, et al., Case No. 30-2014-00701147-CU-NP-CJC (the “Underlying Action”).

17. The complaint alleged that between October 8, 2013 and December 2, 2013, confidential medical records of approximately 32,500 of Cottage’s Hospitals’ patients that were stored electronically on Cottage’s servers were disclosed to the public via the internet.

18. The complaint alleged that the breach occurred because Cottage and/or its third-party vendor, INSYNC Computer Solution, Inc. (“INSYNC”), stored medical records on a system that was fully accessible to the internet but failed to install encryption or take other security measures to protect patient information from becoming available to anyone who “surfed” the internet.

19. The complaint alleged that Cottage violated its nondelegable duties under CMIA and HIPAA to maintain the security of its patients’ confidential medical records and to detect and prevent data breaches on its system that would allow such information to become available to the public through the internet.

20. On or about December 24, 2014, the Court in the Underlying Action granted the class representative’s motion for Preliminary Approval of Proposed Class Action Settlement. The proposed settlement involves creation of a \$4.125 million settlement fund for payments to approximately 50,917 Settlement class members, along with related expenses and attorneys’ fees.

1           21.     Upon information and belief, INSYNC does not maintain sufficient liquid assets  
2 to contribute towards the proposed settlement fund and does not maintain liability insurance  
3 that applies with respect to the privacy claims asserted in the Underlying Action.

4           22.     Columbia incurred more than \$168,000 in defense costs and funded the \$4.125  
5 million settlement of the Underlying Action on behalf of Cottage, subject to a complete  
6 reservation of rights, including the right to seek reimbursement of any funds paid or advanced  
7 on Cottage's behalf pending a resolution of the instant coverage dispute.

8           23.     Columbia also incurred more than \$860,000 in breach and crisis response  
9 expenses on Cottage's behalf, which included attorneys' fees, costs associated with notifying  
10 individuals potentially affected by the breach and the costs of retaining forensics experts to  
11 inspect Cottage's systems and identify the causes of the breach, subject to complete reservation  
12 of rights to recoup such expenses from Cottage.

13  
14  
15 **B.     The California Department of Justice Investigation**

16           24.     The data breach alleged in the Underlying Action is also the subject of a  
17 pending investigation by the California Department of Justice ("DOJ") (the "DOJ  
18 Proceeding"). The DOJ Proceeding will determine whether Cottage complied with its  
19 obligations under HIPAA and any other pertinent state and federal laws and may potentially  
20 result in the imposition of fines, sanctions or penalties.

21  
22 **C.     The Columbia Policy**

23           25.     Columbia issued a "NetProtect360" claims-made liability policy to Cottage in  
24 effect from October 1, 2013 through October 1, 2014, under policy number 425565140-02 (the  
25 "Columbia Policy").  
26  
27  
28

26. As relevant here, the Columbia Policy provides coverage for Privacy Injury Claims and Privacy Regulation Proceedings with limits of \$10,000,000 each claim or proceeding and \$10,000,000 in the aggregate for all Claims – subject to a \$100,000 deductible (the “Columbia Policy.”) Coverage for Privacy Injury Claims is subject to a “Prior Acts” date of May 27, 2012.

27. The Columbia Policy also contains a “Breach Response and Crisis Management Expense Coverage Endorsement” that provides “Breach Response Expense” and “Crisis Management Expense” coverage, subject to a \$5,000,000 limit of insurance.

28. The Columbia Policy contains the following relevant “Liability Coverages” provisions:

A. Insuring Agreements

If the insuring Agreement has been purchased, as indicated in the Declarations, the Insurer will pay on behalf of the Insured all sums in excess of the Deductible and up to the applicable limit of insurance that the Insured shall become legally obligated to pay:

\* \* \*

2. Privacy Injury Liability

A. Privacy Injury Claim

as Damages resulting from any Privacy Injury Claim both first made against the Insured and reported to the Insurer in writing during the Policy Period, or any Extended Reporting Period, if applicable, alleging any Wrongful Act by the insured, or by someone for whose Wrongful Act the Insured is legally responsible;

B. Privacy Regulation Proceeding

as Damages and Claim Expenses resulting from any Privacy Regulation Proceeding both first made against the Insured and reported to the Insurer in writing during the Policy Period, or any Extended Reporting Period, if applicable, alleging any Wrongful Act by the Insured or

1 by someone for whose Wrongful Act the Insured is  
2 legally responsible;...

3 \* \* \*

4 B. Expense Coverages

5 1. Breach Response Expense

6 The Insurer will reimburse the Insured Entity for Breach  
7 Response Expenses (up to the Breach Response Expenses  
8 limit of insurance and in excess of the Breach Response  
9 Event Expenses deductible) incurred within twelve months  
10 of the date that the Insured reports a Security Breach Notice  
11 Law Event.

12 2. Crisis Management Expense

13 The Insurer will reimburse the Insured Entity for Crisis  
14 Management Expenses (up to the Crisis Management  
15 Expenses limit of insurance and in excess of the Crisis  
16 Management Event Expenses deductible) incurred within  
17 twelve months of the date that the Insured reports a Public  
18 Relations Event.

19 29. The Columbia Policy contains the following relevant exclusion:

20 Whether in connection with any First Party Coverage or any  
21 Liability Coverage, the Insurer shall not be liable to pay any Loss:

22 \* \* \*

23 O. Failure to Follow Minimum Required Practices

24 based upon, directly or indirectly arising out of, or in any  
25 way involving:

- 26 1. Any failure of an Insured to continuously implement  
27 the procedures and risk controls identified in the  
28 Insured's application for this Insurance and all related  
information submitted to the Insurer in conjunction  
with such application whether orally or in writing;
2. Failure to follow (in whole or part) any Minimum  
Required Practices that are listed in Minimum Required  
Practices Endorsement; or
3. The Insured's failure to meet any service levels,  
performance standards or metrics;



Item 3 above shall apply only to Insureds whose services are required to satisfy service levels, performance standards or metrics.

This exclusion shall not apply to:

1. an Insured Person's negligent circumvention of controls; or
2. an Insured Person's intentional circumvention of controls where such circumvention was not authorized by the Insured;

30. The Columbia Policy contains a "Healthcare Amendatory Endorsement" that modifies the "Failure to Follow Minimum Required Practices" exclusion as follows:

2. Exclusion O. Failure to Follow Minimum Required Practices, the last subsection that starts with "This exclusion shall not apply to . . ." is deleted in its entirety and replaced with the following:

This exclusion shall not apply to:

1. an Insured Person's negligent circumvention of controls; or
2. an Insured Person's intentional circumvention of controls where such circumvention was not authorized by the Insured;
3. Insured Entity's upgrade or replacement of any procedure or control in item 1 above if the upgraded or replacement procedure or control is at least as effective as the one it replaces.

31. The Columbia Policy contains the following relevant conditions:

I. Application

1. The Insureds represent and acknowledge that the statements contained on the Declarations and in the Application, and any materials submitted or required to be submitted therewith (all of which shall be maintained on file by the Insurer and be deemed attached to and incorporated into this Policy as if physically attached), are the Insured's representations, are true and: (i) are the basis of this Policy and are to be considered as incorporated into and constituting a part of this Policy; and (ii) shall be

deemed material to the acceptance of this risk or the hazard assumed by the Insurer under this Policy. This Policy is issued in reliance upon the truth of such representations.

2. This Policy shall be null and void if the Application contains any misrepresentation or omission:

- a. made with the intent to deceive, or
- b. which materially affects either the acceptance of the risk or the hazard assumed by the Insurer under the Policy.

\* \* \*

Q. Minimum Required Practices

The Insured warrants, as a condition precedent to coverage under this Policy, that it shall:

- 1. follow the Minimum Required Practices that are listed in the Minimum Required Practices endorsement as a condition of coverage under this policy, and
- 2. maintain all risk controls identified in the Insured's Application and any supplemental information provided by the Insured in conjunction with Insured's Application for this Policy.

32. The Columbia Policy contains the following relevant definitions:

Application means all signed applications for this Policy and for any policy in an uninterrupted series of policies issued by the Insurer or any affiliate of the Insurer of which this Policy is a renewal or replacement. Application includes any materials submitted or required to be submitted therewith. An affiliate of the Insurer means an entity controlling, controlled by or under common control with the Insurer.

\* \* \*

Damages means civil awards, settlements and judgments... which the Insureds are legally obligated to pay as a result of a covered Claim. Damages shall not include:

\* \* \*

B. criminal, civil, administrative or regulatory relief, fines or penalties;

\* \* \*

- D. injunctive or declaratory relief;  
E. matters which are uninsurable as a matter of law; or

\* \* \*

Notwithstanding the foregoing paragraph, Damages shall include... punitive, exemplary and multiplied damages. Enforceability of this paragraph shall be governed by such applicable law that most favors coverage for such punitive, exemplary and multiple damages.

\* \* \*

Privacy Regulation Proceeding means a civil, administrative or regulatory proceeding against an Insured by a federal, state or foreign governmental authority alleging violation of any law referenced under the definition of Privacy Injury or a violation of a Security Breach Notice Law.

**D. The Columbia Policy Application**

33. As part of the application submitted in connection with the Columbia Policy, Cottage completed and submitted a "Risk Control Self Assessment" in which it made the following relevant representations:

4. Do you check for security patches to your systems at least weekly and implement them within 30 days? ● Yes
5. Do you replace factory default settings to ensure your information security systems are securely configured? ● Yes
6. Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? ● Yes
11. Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? ● Yes
12. Whenever you entrust sensitive information to 3rd parties do you...
  - a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own ● Yes
  - b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your

standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors) • Yes

c. Audit all such 3rd parties at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? • Yes

d. Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality. • Yes

13. Do you have a way to detect unauthorized access or attempts to access sensitive information? • Yes

23. Do you control and track all changes to your network to ensure it remains secure? • Yes

34. Upon information and belief, Cottage provided false responses to the foregoing questions when applying for coverage from Columbia.

35. Cottage's application for the Columbia Policy contains the following "Warranty":

Applicant hereby declares after inquiry, that the information contained herein and in any supplemental applications or forms required hereby, are true, accurate and complete, and that no material facts have been suppressed or misstated. Applicant acknowledges a continuing obligation to report to the CNA Company to whom this Application is made ("the Company") as soon as practicable any material changes...all such information, after signing the application and prior to issuance of this policy, and acknowledges that the Company shall have the right to withdraw or modify any outstanding quotations and/or authorization or agreement to bind the insurance based upon such changes.

Further, Applicant understands and acknowledges that:

\* \* \*

2) If a policy is issued, the Company will have relied upon, as representations, this application, any supplemental applications and any other statements furnished to this Company in conjunction with this application.

3) All supplemental applications, statements and other materials furnished to the Company in conjunction with this application are hereby incorporated by reference into this application and made a part thereof.

1                   4) This application will be the basis of the contract and will be  
2                   incorporated by referenced into and made a part of such policy.

3                   36. As noted above, the Columbia Policy's "Application" condition memorializes  
4                   Cottage's acknowledgement that the representations made in the application were true, were  
5                   the basis upon which the Columbia Policy was issued, were incorporated by reference within  
6                   the Columbia Policy and were "material to the acceptance of this risk or the hazard assumed by  
7                   the Insurer under this Policy. This Policy is issued in reliance upon the truth of such  
8                   representations."  
9

10                  37. Columbia justifiably relied on the foregoing representations in determining  
11                  whether to issue the Columbia Policy under the terms provided and in determining the  
12                  appropriate premium to be charged.

13                  **E. Claim Investigation**

14                  38. Columbia was originally notified of the data breach issue on December 3, 2013.  
15                  By letter dated January 29, 2014, Columbia acknowledged receipt of the claim and reserved its  
16                  rights under the Columbia Policy. Specifically, Columbia explained that the liability coverage  
17                  provided under the Columbia Policy had not been triggered because Cottage had not yet  
18                  received a demand for monetary damages or notice of a potential regulatory fine associated  
19                  with the data breach and advised Cottage to provide immediate notice upon receipt of any such  
20                  claim. Columbia also reserved rights under the Columbia Policy's Breach Response Expense  
21                  coverage part and assigned counsel to assist Cottage in the breach response process, subject to  
22                  a reservation of rights to assert coverage defenses that arose during Columbia's claim  
23                  investigation.  
24

25                  39. Columbia was then notified of the Underlying Action on January 29, 2014. By  
26                  letter dated February 20, 2014, Columbia supplemented its reservation of rights to address the  
27  
28

1 claims asserted in the Underlying Action. Based on the allegations in the complaint in the  
2 Underlying Action, Columbia reserved the right to disclaim coverage pursuant to the Columbia  
3 Policy's "Failure to Follow Minimum Required Practices" exclusion, among other grounds.

4 40. Columbia thereafter issued further supplemental reservation of rights letters on  
5 July 9, 2014, addressing Cottage's deductible and coinsurance obligations under the Columbia  
6 Policy's Breach Response Expense coverage, and September 17, 2014, addressing additional  
7 and/or alternative coverage defenses that became apparent as its claim investigation proceeded.  
8

9 41. Columbia's claim and coverage investigation revealed that Cottage made a  
10 number of material misrepresentations in the "Risk Control Self Assessment" portion of the  
11 application. By way of example, although Cottage had represented that it "replace[s] factory  
12 default settings to ensure [its] information security systems are securely configured," Columbia  
13 learned of the existence of factory default system configuration settings on Cottage's system  
14 that allowed for anonymous access that had been in place since the server's operating system  
15 was first installed. Columbia also learned of the prevalence of default or missing password  
16 requirements throughout Cottage's network which left its network susceptible to unauthorized  
17 access.  
18  
19

20 42. Although Cottage represented that it checked for "security patches for [its]  
21 systems at least weekly and implement them within 30 days," Columbia learned that Cottage's  
22 system utilized software that was outdated and obsolete to such a degree that security patches  
23 were no longer even available, much less implemented.  
24

25 43. Although Cottage represented that it was equipped to "detect unauthorized  
26 access or attempts to access sensitive information" and that it "track[ed] changes to [its]  
27  
28

1 network to ensure it remains secure,” Columbia learned that Cottage did not maintain any  
2 vulnerability scanner for its system.

3 44. Columbia also learned that Cottage had no enterprise-wide threat management  
4 program and no risk management framework in place prior to the breach, that Cottage did not  
5 regularly conduct risk assessments and that whatever security policies that were in place were  
6 inadequate and were reviewed once every three years. Cottage had represented to Columbia  
7 that it re-assessed its exposure to information security and privacy threats “at least yearly” and  
8 that it enhanced its risk controls as necessary.  
9

10 45. Although Cottage represented that it “enforce[s] a company policy governing  
11 security, privacy and acceptable use of company property that must be followed by anyone  
12 who accesses your network or sensitive information in your care,” Columbia learned that  
13 Cottage did not actually have formal written privacy policies in place at the time of the breach  
14 and Cottage began drafting and implementing such policies only after the breach.  
15

16 46. Although Cottage represented that outsourced its information security  
17 management to a qualified firm, that Cottage performed due diligence with respect to third-  
18 parties entrusted with sensitive information, audited such third-parties yearly to ensure the  
19 adequacy of their safeguards and required such third-parties to maintain sufficient assets or  
20 insurance coverage to respond in the event of a data breach, upon information and belief, the  
21 data breach at issue was contributed to by Cottage’s third-party vendor INSYNC, which lacked  
22 the assets or insurance necessary to contribute towards the settlement of the Underlying  
23 Action. When requested, Cottage failed or refused to provide evidence of its due diligence as  
24 respects its retention of INSYNC or evidence of any audits of INSYNC’s safeguards or  
25 policies.  
26  
27  
28

1           47. Columbia's investigation revealed that the breach was not caused by "an  
2 Insured Person's" negligent or intentional but unauthorized circumvention of controls, or by  
3 Cottage's "upgrade or replacement" of any of the procedures or risk controls described in the  
4 application but, rather, by the complete absence of any such risk controls in the first instance.

5           48. Since Columbia's coverage investigation was on-going, prior to funding the  
6 \$4.125 million settlement of the Underlying Action, Columbia advised Cottage that its  
7 agreement to fund the settlement was made subject to a full and complete reservation of rights  
8 under the Columbia Policy and applicable law to disclaim coverage and seek reimbursement in  
9 full from Cottage for any and all amounts paid towards settlement of the Underlying Action,  
10 along with any and all attorney's fees or related costs and breach response expenses Columbia  
11 has paid or will pay in connection with the breach.  
12

13           49. Following its agreement to fund the settlement of the Underlying Action  
14 pursuant to a reservation of rights, Columbia attempted to conduct negotiations with Cottage to  
15 explore whether a global resolution of the coverage issues could be reached. This effort was  
16 unsuccessful.  
17

18           50. In light of the Columbia Policy's alternative dispute resolution ("ADR")  
19 provision, which required participation in either non-binding mediation or arbitration prior to  
20 the commencement of suit, Columbia also proposed that the parties participate in mediation or  
21 arbitration. Cottage advised that it would not participate in arbitration and that mediation  
22 would be futile because Cottage would not agree to Columbia's settlement parameters.  
23

24           51. Accordingly, counsel for Columbia advised counsel for Cottage of Columbia's  
25 intent to proceed with the commencement of litigation and forwarded counsel a courtesy copy  
26  
27  
28



1 of its declaratory judgment complaint. Counsel for Cottage did not object or respond to  
2 Columbia's continued efforts to discuss a possible expedited resolution of the matter.

3 **F. The Prior Declaratory Judgment Action**

4 52. On May 7, 2015, Columbia commenced an action against Cottage in the District  
5 Court for the Central District of California (Case No.: 2:15-cv-03432) seeking a declaration  
6 that it is not obligated to provide Cottage with a defense or indemnification in connection with  
7 any claims stemming from the data breach at issue, as well as a declaration of its entitlement to  
8 reimbursement of all amounts Columbia advanced in connection with the data breach.  
9

10 53. On June 18, 2015, Cottage moved to dismiss the action for lack of subject  
11 matter jurisdiction pursuant to the Columbia Policy's ADR provision.  
12

13 54. By order dated July 17, 2015, the Court granted Cottage's motion dismissing  
14 the action without prejudice pending the parties' participation in the ADR process.

15 55. The parties subsequently participated in mediation of this matter on February  
16 12, 2016, which was unsuccessful.  
17

18 56. More than sixty (60 days) have elapsed since the termination of said mediation.  
19 As such, Columbia has satisfied the Columbia Policy's ADR provision and may proceed with  
20 the instant action.

21 57. A dispute remains concerning the existence and scope of any obligation on the  
22 part of Columbia to Cottage under the Columbia Policy in connection with the claims at issue  
23 in the Underlying Action and the DOJ Proceeding.  
24

25 58. Columbia seeks declaration that coverage under the Columbia Policy does not  
26 apply to the data breach at issue, that Columbia has no duty to defend or indemnify Cottage in  
27 the Underlying Action or the DOJ Proceeding.  
28

1           59.     Additionally, in light of certain facts discovered during the course of  
2 Columbia's claim investigation, Cottage made certain material misrepresentations and/or  
3 omissions of fact when applying for coverage under the Columbia Policy rendering the policy  
4 void *ab initio* and subject to rescission. Columbia seeks a declaration of its entitlement to same.

5           60.     Therefore, an actual and justiciable controversy exists regarding the nature and  
6 scope of the insurance coverage potentially owed to Cottage.  
7

8                           **FIRST CAUSE OF ACTION**

9                                   **(Declaratory Relief)**

10           61.     Columbia repeats, reiterates and realleges each and every allegation of the  
11 preceding paragraphs as if set forth herein, verbatim and fully at length.  
12

13           62.     The Columbia Policy contains an exclusion entitled "Failure to Follow  
14 Minimum Required Practices" that precludes coverage for any loss based upon, directly or  
15 indirectly arising out of, or in any way involving "[a]ny failure of an Insured to continuously  
16 implement the procedures and risk controls identified in the Insured's application for this  
17 Insurance and all related information submitted to the Insurer in conjunction with such  
18 application whether orally or in writing."  
19

20           63.     Upon information and belief, the data breach at issue in the Underlying Action  
21 and the DOJ Proceeding was caused as a result of File Transfer Protocol settings on Cottage's  
22 internet servers that permitted anonymous user access, thereby allowing electronic personal  
23 health information to become available to the public via Google's internet search engine.  
24

25           64.     Upon information and belief, the data breach at issue in the Underlying Action  
26 and the DOJ Proceeding was caused by Cottage's failure to continuously implement the  
27 procedures and risk controls identified in its application, including, but not limited to, its  
28

1 failure to replace factory default settings and its failure to ensure that its information security  
2 systems were securely configured, among other things.

3 65. Upon information and belief, the data breach at issue in the Underlying Action  
4 and the DOJ Proceeding was caused by Cottage's failure to regularly check and maintain  
5 security patches on its systems, its failure to regularly re-assess its information security  
6 exposure and enhance risk controls, its failure to have a system in place to detect unauthorized  
7 access or attempts to access sensitive information stored on its servers and its failure to control  
8 and track all changes to its network to ensure it remains secure, among other things.

10 66. Upon information and belief, the data breach at issue in the Underlying Action  
11 and the DOJ Proceeding did not arise from "an Insured Person's negligent circumvention of  
12 controls; an Insured Person's intentional circumvention of controls where such circumvention  
13 was not authorized by the Insured; [or] Insured Entity's upgrade or replacement of any  
14 procedure or control in item 1 above if the upgraded or replacement procedure or control is at  
15 least as effective as the one it replaces" within the meaning of the exceptions to the Failure to  
16 Follow Minimum Required Practices exclusion set forth in the Columbia Policy's Healthcare  
17 Amendatory Endorsement.

20 67. Accordingly, Columbia is entitled to a declaration that coverage under the  
21 Columbia Policy does not apply to the data breach at issue, that Columbia is not obligated to  
22 defend or indemnify Cottage in connection with the Underlying Action or the DOJ Proceeding  
23 and that coverage for the claims and potential damages at issue in the Underlying Action and  
24 the DOJ Proceeding is precluded pursuant to the Columbia Policy's Failure to Follow  
25 Minimum Required Practices exclusion.  
26  
27  
28

**SECOND CAUSE OF ACTION**

**(Declaratory Relief)**

68. Columbia repeats, reiterates and realleges each and every allegation of the preceding paragraphs as if set forth herein, verbatim and fully at length.

69. The Columbia Policy's insuring agreement for a Privacy Regulation Proceeding applies with respect to Cottage's liability for "Damages and Claim Expenses resulting from any Privacy Regulation Proceeding."

70. The term "Damages" is defined under the Columbia Policy to mean "civil awards, settlements and judgments... which the Insureds are legally obligated to pay as a result of a covered Claim," but does not include "criminal, civil, administrative or regulatory relief, fines or penalties."

71. The DOJ Proceeding will determine whether Cottage complied with its obligations under HIPAA and any other pertinent state and federal laws and may result in the imposition of civil, administrative or regulatory relief, fines or penalties against Cottage.

72. Accordingly, Columbia is entitled to a declaration that it is not obligated to defend or indemnify Cottage in connection with the DOJ Proceeding as any sanctions imposed or other relief awarded or in the DOJ Proceeding would not involve covered Damages under the Columbia Policy.

**THIRD CAUSE OF ACTION**

**(Declaratory Relief)**

73. Columbia repeats, reiterates and realleges each and every allegation of the preceding paragraphs as if set forth herein, verbatim and fully at length.

1           74. The Columbia Policy's "Application" condition provides that the Columbia  
2 Policy "shall be null and void if the Application contains any misrepresentation or omission: a.  
3 made with the intent to deceive, or b. which materially affects either the acceptance of the risk  
4 or the hazard assumed by the Insurer under the Policy."

5           75. The Columbia Policy's "Minimum Required Practices" condition provides that,  
6 as a "condition precedent to coverage," Cottage warrants that it shall "maintain all risk controls  
7 identified in the Insured's Application and any supplemental information provided by the  
8 Insured in conjunction with Insured's Application for this Policy."

9  
10           76. Upon information and belief, Cottage's application for coverage under the  
11 Columbia Policy contained misrepresentations and/or omissions of material fact that were  
12 made negligently or with intent to deceive concerning Cottage's data breach risk controls.

13  
14           77. Upon information and belief, the data breach at issue in the Underlying Action  
15 and the DOJ Proceeding was caused by Cottage's failure to maintain the risk controls  
16 identified in its application, including, but not limited to, its failure to replace factory default  
17 settings to ensure that its information security systems were securely configured.

18  
19           78. Accordingly, Columbia is entitled to a declaration that coverage under the  
20 Columbia Policy does not apply to the data breach at issue, that Columbia is not obligated to  
21 defend or indemnify Cottage in connection with the Underlying Action or the DOJ Proceeding  
22 based on Cottage's breaches of the Columbia Policy's "Application" and "Minimum Required  
23 Practices" conditions.  
24

25                           **FOURTH CAUSE OF ACTION**

26                                   **(Rescission)**

1           79. Columbia repeats, reiterates and realleges each and every allegation of the  
2 preceding paragraphs as if set forth herein, verbatim and fully at length

3           80. Upon information and belief, Cottage made misrepresentations and/or omissions  
4 of material fact concerning its data breach risk controls when applying for coverage under the  
5 Columbia Policy.  
6

7           81. Upon information and belief, Cottage misrepresented the fact that it replaced  
8 factory default settings to ensure that its information security systems were securely  
9 configured.  
10

11           82. Upon information and belief, Cottage misrepresented the facts that it regularly  
12 checked and maintained security patches on its systems, that it regularly re-assessed its  
13 information security exposure and enhanced risk controls, that it had a system in place to detect  
14 unauthorized access or attempts to access sensitive information stored on its servers and that it  
15 controlled and tracked all changes to its network to ensure it remains secure, among other  
16 things.  
17

18           83. Upon information and belief, Cottage made misrepresentations regarding the  
19 firm or other third parties to which Cottage outsourced its information security management,  
20 the degree of due diligence Cottage exercised with respect to said third party's safeguards and  
21 audits performed regarding the same, among other things.  
22

23           84. Cottage made the foregoing misrepresentations and/or omissions of material  
24 fact with the full knowledge and expectation that Columbia would rely on said representations,  
25 which were a material and critical part of Columbia's consideration of the risk and  
26 determination to issue the Columbia Policy under the terms provided and for the premium  
27 charged.  
28

1 85. Columbia justifiably relied on the representations made in Cottage's insurance  
2 application in determining whether to issue the Columbia Policy under the terms provided and  
3 in determining the appropriate premium to be charged.

4 86. If the true facts had been known, Columbia would not have issued the Columbia  
5 Policy and/or would not have provided coverage under the same terms or with respect to the  
6 hazard resulting in the claims at issue.

7  
8 87. Therefore, Columbia is entitled to a declaration that the Columbia Policy is  
9 rescinded and void *ab initio*. Columbia also is entitled to an Order permitting it to return to  
10 Cottage the premium paid in connection with the Columbia Policy.

11  
12 **FIFTH CAUSE OF ACTION**

13 **(Reimbursement of Defense, Expense and Settlement Payments)**

14 88. Columbia repeats, reiterates and realleges each and every allegation of the  
15 preceding paragraphs as if set forth herein, verbatim and fully at length.

16 89. Columbia agreed to incur breach response expenses on Cottage's behalf, to  
17 participate in Cottage's defense in the Underlying Action and to fund the \$4.125 million  
18 settlement of the Underlying Action subject to a complete reservation of rights, including the  
19 right to seek reimbursement of any funds paid or advanced on Cottage's behalf pending a  
20 resolution of the instant coverage dispute.

21  
22 90. To the extent that the Columbia Policy does not provide coverage for the data  
23 breach at issue and the claims asserted in the Underlying Action and/or to the extent that the  
24 Columbia Policy is subject to rescission, Columbia is entitled to reimbursement from Cottage  
25 for the full amount of the \$4.125 million Columbia paid in settlement of the Underlying  
26 Action, along with any and all defense costs, attorney's fees or related costs and data breach  
27  
28

1 response expenses incurred by Columbia on Cottage's behalf, pursuant to Blue Ridge Ins. Co.  
2 v. Jacobsen, 25 Cal 4th 489 (2001); See also Axis Surplus Ins. Co. v. Reinoso, 208 Cal App  
3 4th 181 (Cal Ct App 2012).

4 **WHEREFORE**, Plaintiff, Columbia Casualty Company, prays for the following relief:

- 5 (a) For a declaration that Columbia is not obligated to provide Cottage with coverage  
6 for any costs or breach response expenses incurred in connection with the data  
7 breach at issue or any damages awarded, sanctions imposed or any other relief  
8 directed in the Underlying Action and the DOJ Proceeding;
- 9 (b) For a declaration that Columbia is not obligated to provide Cottage with coverage  
10 for any defense costs or claim expenses incurred in connection with the  
11 Underlying Action and the DOJ Proceeding;
- 12 (c) For a declaration that the Columbia Policy is rescinded and void *ab initio* and  
13 permitting Columbia to return to Cottage the premium paid in connection with the  
14 Columbia Policy;
- 15 (d) For a declaration that Cottage is obligated to reimburse Columbia for any and all  
16 sums Columbia paid on Cottage's behalf in connection with the Underlying  
17 Action, along with any and all defense costs, attorney's fees or related costs or  
18 expenses incurred by Columbia on Cottage's behalf, including, but not limited to,  
19 the \$4.125 million settlement, related defense costs exceeding \$168,000 and data  
20 breach response expenses exceeding \$860,000;
- 21 (e) For an award of Columbia's attorneys' fees and costs pursuant to law; and
- 22 (f) For such other relief as is just and equitable herein.

23 Dated: May 31, 2016

24 CARROLL, McNULTY & KULL LLC

25 BY: /s/ Matthew T. Walsh  
26 Matthew T. Walsh, Esq.  
27 Attorneys for Plaintiff  
28 100 North Riverside Plaza, Suite 2100  
Chicago, Illinois 60606  
(312) 800-5000 (tel.)  
(312) 800-5010 (fax)  
mwalsh@cmk.com



UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**I. (a) PLAINTIFFS** ( Check box if you are representing yourself ☐ )

Columbia Casualty Company

**DEFENDANTS** ( Check box if you are representing yourself ☐ )

Cottage Health System

(b) County of Residence of First Listed Plaintiff Cook County, IL

(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Santa Barbara, CA

(IN U.S. PLAINTIFF CASES ONLY)

(c) Attorneys (Firm Name, Address and Telephone Number) If you are representing yourself, provide the same information.

Carroll, McNulty & Kull LLC  
100 North Riverside Plaza, Suite 2100  
Chicago, Illinois 60606  
Telephone: (312) 800-5000

Attorneys (Firm Name, Address and Telephone Number) If you are representing yourself, provide the same information.

**II. BASIS OF JURISDICTION** (Place an X in one box only.)

- ☐ 1. U.S. Government Plaintiff
- ☐ 2. U.S. Government Defendant
- ☐ 3. Federal Question (U.S. Government Not a Party)
- ☒ 4. Diversity (Indicate Citizenship of Parties in Item III)

**III. CITIZENSHIP OF PRINCIPAL PARTIES**-For Diversity Cases Only  
(Place an X in one box for plaintiff and one for defendant)

- |   | PTF                                   | DEF                                   |   | PTF                        | DEF                                   |
|---|---------------------------------------|---------------------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State                   | <input type="checkbox"/> 1            | <input checked="" type="checkbox"/> 1 | Incorporated or Principal Place of Business in this State     | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State                | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2            | Incorporated and Principal Place of Business in Another State | <input type="checkbox"/> 5 | <input checked="" type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3            | <input type="checkbox"/> 3            | Foreign Nation  | <input type="checkbox"/> 6 | <input type="checkbox"/> 6            |

**IV. ORIGIN** (Place an X in one box only.)

- ☒ 1. Original Proceeding ☐ 2. Removed from State Court ☐ 3. Remanded from Appellate Court ☐ 4. Reinstated or Reopened ☐ 5. Transferred from Another District (Specify) ☐ 6. Multi-District Litigation

**V. REQUESTED IN COMPLAINT: JURY DEMAND:** ☐ Yes ☒ No (Check "Yes" only if demanded in complaint.)**CLASS ACTION under F.R.Cv.P. 23:** ☐ Yes ☒ No **MONEY DEMANDED IN COMPLAINT:** \$ \$4.125 million**VI. CAUSE OF ACTION** (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)

Declaratory Judgment pursuant to 28 U.S.C. §2201 and Reimbursement of Defense and Settlement Payments.

**VII. NATURE OF SUIT** (Place an X in one box only.)

OTHER STATUTES	CONTRACT	REAL PROPERTY CONT.	IMMIGRATION	PRISONER PETITIONS	PROPERTY RIGHTS
<input type="checkbox"/> 375 False Claims Act	<input checked="" type="checkbox"/> 110 Insurance	<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 462 Naturalization Application	<b>Habeas Corpus:</b>	<input type="checkbox"/> 820 Copyrights
<input type="checkbox"/> 400 State Reapportionment	<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 463 Alien Detainee	<input type="checkbox"/> 830 Patent
<input type="checkbox"/> 410 Antitrust	<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 290 All Other Real Property	<b>TORTS</b>	<input type="checkbox"/> 510 Motions to Vacate Sentence	<input type="checkbox"/> 840 Trademark
<input type="checkbox"/> 430 Banks and Banking	<input type="checkbox"/> 140 Negotiable Instrument	<b>PERSONAL INJURY</b>	<b>PERSONAL PROPERTY</b>	<input type="checkbox"/> 530 General	<b>SOCIAL SECURITY</b>
<input type="checkbox"/> 450 Commerce/ICC Rates/Etc.	<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 370 Other Fraud	<input type="checkbox"/> 535 Death Penalty	<input type="checkbox"/> 861 HIA (1395ff)
<input type="checkbox"/> 460 Deportation	<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 315 Airplane Product Liability	<input type="checkbox"/> 371 Truth in Lending	<b>Other:</b>	<input type="checkbox"/> 862 Black Lung (923)
<input type="checkbox"/> 470 Racketeer Influenced & Corrupt Org.	<input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Vet.)	<input type="checkbox"/> 320 Assault, Libel & Slander	<input type="checkbox"/> 380 Other Personal Property Damage	<input type="checkbox"/> 540 Mandamus/Other	<input type="checkbox"/> 863 DIWC/DIWW (405 (g))
<input type="checkbox"/> 480 Consumer Credit	<input type="checkbox"/> 153 Recovery of Overpayment of Vet. Benefits	<input type="checkbox"/> 330 Fed. Employers' Liability	<input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 550 Civil Rights	<input type="checkbox"/> 864 SSID Title XVI
<input type="checkbox"/> 490 Cable/Sat TV	<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 340 Marine	<b>BANKRUPTCY</b>	<input type="checkbox"/> 555 Prison Condition	<input type="checkbox"/> 865 RSI (405 (g))
<input type="checkbox"/> 850 Securities/Commodities/Exchange	<input type="checkbox"/> 190 Other Contract	<input type="checkbox"/> 345 Marine Product Liability	<input type="checkbox"/> 422 Appeal 28 USC 158	<input type="checkbox"/> 560 Civil Detainee Conditions of Confinement	<b>FEDERAL TAX SUITS</b>
<input type="checkbox"/> 890 Other Statutory Actions	<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 350 Motor Vehicle	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<b>FORFEITURE/PENALTY</b>	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)
<input type="checkbox"/> 891 Agricultural Acts	<input type="checkbox"/> 196 Franchise	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<b>CIVIL RIGHTS</b>	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	<input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
<input type="checkbox"/> 893 Environmental Matters	<b>REAL PROPERTY</b>	<input type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 440 Other Civil Rights	<b>LABOR</b>	
<input type="checkbox"/> 895 Freedom of Info. Act	<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 362 Personal Injury-Med Malpractice	<input type="checkbox"/> 441 Voting	<input type="checkbox"/> 710 Fair Labor Standards Act	
<input type="checkbox"/> 896 Arbitration	<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 365 Personal Injury-Product Liability	<input type="checkbox"/> 442 Employment	<input type="checkbox"/> 720 Labor/Mgmt. Relations	
<input type="checkbox"/> 899 Admin. Procedures Act/Review of Appeal of Agency Decision	<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability	<input type="checkbox"/> 443 Housing/Accommodations	<input type="checkbox"/> 740 Railway Labor Act	
<input type="checkbox"/> 950 Constitutionality of State Statutes		<input type="checkbox"/> 368 Asbestos Personal Injury Product Liability	<input type="checkbox"/> 445 American with Disabilities-Employment	<input type="checkbox"/> 751 Family and Medical Leave Act	
			<input type="checkbox"/> 446 American with Disabilities-Other	<input type="checkbox"/> 790 Other Labor Litigation	
			<input type="checkbox"/> 448 Education	<input type="checkbox"/> 791 Employee Ret. Inc. Security Act	

FOR OFFICE USE ONLY:

Case Number:

CV-71 (10/14)

CIVIL COVER SHEET

Page 1 of 3

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**

**VIII. VENUE:** Your answers to the questions below will determine the division of the Court to which this case will be initially assigned. This initial assignment is subject to change, in accordance with the Court's General Orders, upon review by the Court of your Complaint or Notice of Removal.

<b>QUESTION A: Was this case removed from state court?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "no," skip to Question B. If "yes," check the box to the right that applies, enter the corresponding division in response to Question E, below, and continue from there.	STATE CASE WAS PENDING IN THE COUNTY OF:		INITIAL DIVISION IN CACD IS:
	<input type="checkbox"/> Los Angeles, Ventura, Santa Barbara, or San Luis Obispo		Western
	<input type="checkbox"/> Orange		Southern
	<input type="checkbox"/> Riverside or San Bernardino		Eastern

<b>QUESTION B: Is the United States, or one of its agencies or employees, a PLAINTIFF in this action?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "no," skip to Question C. If "yes," answer Question B.1, at right.	<b>B.1.</b> Do 50% or more of the defendants who reside in the district reside in Orange Co.?  <i>check one of the boxes to the right</i> ➔	<input type="checkbox"/> YES. Your case will initially be assigned to the Southern Division. Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question B.2.
<b>B.2.</b> Do 50% or more of the defendants who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)  <i>check one of the boxes to the right</i> ➔	<input type="checkbox"/> YES. Your case will initially be assigned to the Eastern Division. Enter "Eastern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Your case will initially be assigned to the Western Division. Enter "Western" in response to Question E, below, and continue from there.	

<b>QUESTION C: Is the United States, or one of its agencies or employees, a DEFENDANT in this action?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "no," skip to Question D. If "yes," answer Question C.1, at right.	<b>C.1.</b> Do 50% or more of the plaintiffs who reside in the district reside in Orange Co.?  <i>check one of the boxes to the right</i> ➔	<input type="checkbox"/> YES. Your case will initially be assigned to the Southern Division. Enter "Southern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Continue to Question C.2.
<b>C.2.</b> Do 50% or more of the plaintiffs who reside in the district reside in Riverside and/or San Bernardino Counties? (Consider the two counties together.)  <i>check one of the boxes to the right</i> ➔	<input type="checkbox"/> YES. Your case will initially be assigned to the Eastern Division. Enter "Eastern" in response to Question E, below, and continue from there.  <input type="checkbox"/> NO. Your case will initially be assigned to the Western Division. Enter "Western" in response to Question E, below, and continue from there.	

QUESTION D: Location of plaintiffs and defendants?	A. Orange County	B. Riverside or San Bernardino County	C. Los Angeles, Ventura, Santa Barbara, or San Luis Obispo County
Indicate the location(s) in which 50% or more of <i>plaintiffs who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Indicate the location(s) in which 50% or more of <i>defendants who reside in this district</i> reside. (Check up to two boxes, or leave blank if none of these choices apply.)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

<b>D.1. Is there at least one answer in Column A?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "yes," your case will initially be assigned to the SOUTHERN DIVISION. Enter "Southern" in response to Question E, below, and continue from there. If "no," go to question D2 to the right.     ➔	<b>D.2. Is there at least one answer in Column B?</b> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If "yes," your case will initially be assigned to the EASTERN DIVISION. Enter "Eastern" in response to Question E, below. If "no," your case will be assigned to the WESTERN DIVISION. Enter "Western" in response to Question E, below.     ↓
---	---

QUESTION E: Initial Division?	INITIAL DIVISION IN CACD
Enter the initial division determined by Question A, B, C, or D above: ➔	Western

QUESTION F: Northern Counties?
Do 50% or more of plaintiffs or defendants in this district reside in Ventura, Santa Barbara, or San Luis Obispo counties? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA  
CIVIL COVER SHEET**IX(a). IDENTICAL CASES:** Has this action been previously filed in this court?☒ NO☐ YES

If yes, list case number(s): \_\_\_\_\_

**IX(b). RELATED CASES:** Is this case related (as defined below) to any civil or criminal case(s) previously filed in this court?☒ NO☐ YES

If yes, list case number(s): \_\_\_\_\_

**Civil cases** are related when they (check all that apply):

- ☐ A. Arise from the same or a closely related transaction, happening, or event;
- ☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
- ☐ C. For other reasons would entail substantial duplication of labor if heard by different judges.

Note: That cases may involve the same patent, trademark, or copyright is not, in itself, sufficient to deem cases related.

**A civil forfeiture case and a criminal case** are related when they (check all that apply):

- ☐ A. Arise from the same or a closely related transaction, happening, or event;
- ☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
- ☐ C. Involve one or more defendants from the criminal case in common and would entail substantial duplication of labor if heard by different judges.

**X. SIGNATURE OF ATTORNEY****(OR SELF-REPRESENTED LITIGANT):** /s/ Matthew T. WalshDATE: May 30, 2016

**Notice to Counsel/Parties:** The submission of this Civil Cover Sheet is required by Local Rule 3-1. This Form CV-71 and the information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. For more detailed instructions, see separate instruction sheet (CV-071A).

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405 (g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405 (g))

2016 WL 3055111

Only the Westlaw citation is currently available.  
United States District Court, D. Arizona.

P.F. CHANG'S CHINA  
BISTRO, INC., Plaintiff,  
v.  
FEDERAL INSURANCE  
COMPANY, Defendant.

No. CV-15-01322-PHX-SMM

Signed 05/26/2016

Filed 05/31/2016

**Attorneys and Law Firms**

[Anthony W. Merrill](#), [Emerson Tanner Warnick](#),  
[Troy Blinn Froderman](#), Polsinelli PC, Phoenix, AZ,  
for Plaintiff.

[Kevin Richard Myer](#), [Robert Thomas Aquinas Sullivan](#),  
Broening Oberg Woods & Wilson PC, Phoenix, AZ,  
[David Newmann](#), Hogan Lovells US LLP, Philadelphia, PA,  
[Ellen S. Kennedy](#), Hogan Lovells US LLP, Washington, DC, for Defendant.

**ORDER**

Honorable [Stephen M. McNamee](#), Senior United States District Judge

\*1 Pending before the Court is Defendant Federal Insurance Company's ("Federal") Motion for Summary Judgment. (Doc. 22.) P.F. Chang's China Bistro, Inc. ("Chang's") has responded and the matter is fully briefed. (Docs. 36, 38.) The Court heard Oral Arguments on the motion on April 19, 2016. (Doc. 41.) In essence, the main issue before the Court is whether coverage exists under the insurance policy between Chang's and Federal for the credit card association assessments that arose from the data breach Chang's suffered in 2013. The Court now issues following ruling.

**I. FACTUAL BACKGROUND**<sup>1</sup>**A. The CyberSecurity Insurance Policy**

Federal sold a CyberSecurity by Chubb Policy ("Policy") to Chang's corporate parent, Wok Holdco LLC, with effective dates from January 1, 2014 to January 1, 2015. (Doc. 8-1 at 2.) On its website, Federal marketed the Policy as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world" that "[c]overs direct loss, legal liability, and consequential loss resulting from cyber security breaches." (Doc. 37-7.) Specific provisions of the Policy will be defined and discussed in greater detail below.

During the underwriting processes, Federal classified Chang's as a high risk, "PCI Level 1", client because Chang's conducts more than 6 million transactions per year. (Docs. 37-1 at 121-22, 37-6.) Further, because of the large number of Chang's transactions conducted with customer credit cards, Federal noted there was high exposure to potential customer identity theft. (Doc. 37-6.) In 2014, Chang's paid an annual premium of \$134,052.00 for the Policy. (Doc. 37-1 at 126.)

**B. The Master Service Agreement Between Chang's and BAMS**

Chang's and other similarly situated merchants are unable to process credit card transactions themselves. Merchants must enter into agreements with third-party "Servicers" or "Acquirers" who facilitate the processing of credit card transactions with the banks who issue the credit cards ("Issuers"), such as Chase or Wells Fargo. Here, Chang's entered into a Master Service Agreement ("MSA") with Bank of America Merchant Services ("BAMS") to process credit card payments made by Chang's customers. (Doc. 23-2.) Under the MSA, Chang's delivers its customers' credit card payment information to BAMS who then settles the transaction through an automated clearinghouse; BAMS then credits Chang's account for the amount of the payment. (*Id.*)

Servicers like BAMS perform their processing obligations pursuant to agreements with the credit card associations ("Associations"), like

MasterCard and Visa. (Doc. 24-1.) BAMS' agreement with MasterCard is governed by the MasterCard Rules, and are incorporated in its MSA with Chang's. (See Id.; Doc. 23-2.) Under the MasterCard Rules, BAMS is obligated to pay certain fees and assessments ("Assessments") to MasterCard in the event of a data breach or "Account Data Compromise" ("ADC"). (Doc. 24-1 at § 10.2) These Assessments include "Operational Reimbursement" fees and "Fraud Recovery" fees, and they are calculated by formulae set forth in the MasterCard Rules. (Id.)

\*2 Under the MSA, Chang's agreed to compensate or reimburse BAMS for "fees," "fines," "penalties," or "assessments" imposed on BAMS by the Associations. (See Doc. 23-2 at 9, 18.) Section 13.5 of the Addendum to the MSA reads: "[Chang's] agrees to pay [BAMS] any fines, fees, or penalties imposed on [BAMS] by any Associations, resulting from Chargebacks and any other fines, fees or penalties imposed by an Association with respect to acts or omissions of [Chang's]." (Id. at 9.) Section 5 of Schedule A to the Addendum to the MSA provides: "In addition to the interchange rates, [BAMS] may pass through to [Chang's] any fees assessed to [BAMS] by the [Associations], including but not limited to, new fees, fines, penalties and assessments imposed by the [Associations]." (Id. at 18.)

### C. The Security Compromise

On June 10, 2014, Chang's learned that computer hackers had obtained and posted on the Internet approximately 60,000 credit card numbers belonging to its customers (the "security compromise" or "data breach"). (Doc. 25-1.) Chang's notified Federal of the data breach that very same day. (Id.)

To date, Federal has reimbursed Chang's more than \$1,700,000 pursuant to the Policy for costs incurred as a result of the security compromise. (Doc. 22 at 9.) Those costs include conducting a forensic investigation into the data breach and the costs of defending litigation filed by customers whose credit card information was stolen, as well as litigation filed by one bank that issued card information that was stolen. (Id.)

Following the data breach, on March 2, 2015, MasterCard issued an "ADC Operational Reimbursement/Fraud Recovery Final Acquirer Financial Responsibility Report" to BAMS. (Doc. 26-2.) This MasterCard Report imposed three Assessments on BAMS, a Fraud Recovery Assessment of \$1,716,798.85, an Operational Reimbursement Assessment of \$163,122.72 for Chang's data breach, and a Case Management Fee of \$50,000. (Id.; Doc. 26-3.) The Fraud Recovery Assessment reflects costs, as calculated by MasterCard, associated with fraudulent charges that may have arisen from, or may be related to, the security compromise. (Doc. 1-1 at ¶20.) The Operational Reimbursement Assessment reflects costs to notify cardholders affected by the security compromise and to reissue and deliver payment cards, new account numbers, and security codes to those cardholders. (Id. at ¶19) The Case Management Fee is a flat fee and relates to considerations regarding Chang's compliance with Payment Card Industry Data Security Standards. (Id. at ¶18.)

### D. The BAMS Letter

On March 11, 2015, BAMS sent Chang's a letter (the "BAMS Letter") stating:

MasterCard's investigation concerning the account data compromise event involving [Chang's] is now complete. [BAMS] has been notified by MasterCard that a case management fee and Account Data Compromise (ADC) Operational Reimbursement and Fraud Recovery (ORFR) are being assessed against [BAMS] as a result of the data compromise. In accordance with your [MSA] you are obligated to reimburse [BAMS] for the following assessments:

- \$ 50,000.00 – Case Management Fee
- \$ 163,122.72 – ADC Operational Reimbursement
- \$1,716,798.85 – ADC Fraud Recovery

\$1,929,921.57<sup>2</sup>



(Doc. 26-3.) Chang's notified Federal of the BAMS Letter on March 19, 2015 and sought coverage for the Assessments. (Doc. 26-4.) Pursuant to the MSA, and in order to continue operations and not lose its ability to process credit card transactions, Chang's reimbursed BAMS for the Assessments on April 15, 2015. (Doc. 1-1 at ¶24.) Federal denied coverage for the Assessments and Chang's subsequently filed this lawsuit.

## II. STANDARD OF REVIEW

"The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." [Fed.R.Civ.P. 56\(a\)](#). "The substantive law determines which facts are material; only disputes over facts that might affect the outcome of the suit under the governing law properly preclude the entry of summary judgment." [Nat'l Ass'n of Optometrists & Opticians v. Harris](#), 682 F.3d 1144, 1147 (9th Cir. 2012) (citing [Anderson v. Liberty Lobby, Inc.](#), 477 U.S. 242, 248 (1986)). To prove the absence of a genuine dispute, the moving party must demonstrate that "the evidence is such that [no] reasonable jury could return a verdict for the nonmoving party." [Liberty Lobby](#), 477 U.S. at 248. In determining whether a party has met its burden, a court views the evidence in the light most favorable to the non-moving party and draws all reasonable inferences in the non-moving party's favor. [Liberty Lobby](#), 477 U.S. at 255. While a court may consider only admissible evidence in ruling on a motion for summary judgment, the focus is not "on the admissibility of the evidence's form," but "on the admissibility of its contents." [Fraser v. Goodale](#), 342 F.3d 1032, 1036–37 (9th Cir. 2003).

\*3 Federal courts sitting in diversity apply the forum state's choice of law rules to determine controlling substantive law. [Klaxon Co. v. Stentor Elec. Mfg. Co. Inc.](#), 313 U.S. 487, 496 (1941). Arizona adheres to [Restatement \(Second\) of Conflict of Laws § 193](#) (1971), which states that insurance contracts are generally governed "by the local law of the state which the parties understood was to be the principal location of the insured risk during the term of the policy." [Beckler v. State](#)

[Farm Mut. Auto. Ins. Co.](#), 195 Ariz. 282, 286, 987 P.2d 768, 772 (App. 1999). Since the principal location of the insured was in Arizona and the insurance agreement was entered into in Arizona, Arizona law governs the enforcement of the Policy.

"The traditional view of the law of contracts is that a written agreement adopted by the parties will be viewed as an integrated contract which binds those parties to the terms expressed within the four corners of the agreement." [Darner Motor Sales, Inc. v. Universal Underwriters Ins. Co.](#), 140 Ariz. 383, 390, 682 P.2d 388, 395 (1984). However, "the usual insurance policy is a special kind of contract," *id.*, in part because it is not "arrived at by negotiation between the parties," [Zuckerman v. Transamerica Ins. Co.](#), 133 Ariz. 139, 144, 650 P.2d 441, 446 (1982). Instead, "[i]t is largely adhesive; some terms are bargained for, but most terms consist of boilerplate, not bargained for, neither read nor understood by the buyer, and often not even fully understood by the selling agent." [Darner](#), 140 Ariz. at 391, 682 P.2d at 396. Moreover, "[t]he adhesive terms generally are self-protective; their major purpose and effect often is to ensure that the drafting party will prevail if a dispute goes to court." [Gordinier v. Aetna Cas. & Sur. Co.](#), 154 Ariz. 266, 271, 742 P.2d 277, 282 (1987). Accordingly, "special contract rules should apply." *Id.*

Interpretation of insurance policies is a question of law. [Sparks v. Republic Nat. Life Ins. Co.](#), 132 Ariz. 529, 534, 647 P.2d 1127, 1132 (1982). "Provisions of insurance policies are to be construed in a manner according to their plain and ordinary meaning," *id.*, but if a clause is reasonably susceptible to different interpretations given the facts of the case, the clause is to be construed "by examining the language of the clause, public policy considerations, and the purpose of the transaction as a whole," [State Farm Mut. Auto. Ins. Co. v. Wilson](#), 162 Ariz. 251, 257, 782 P.2d 727, 733 (1989). "[T]he general rule is that while coverage clauses are interpreted broadly so as to afford maximum coverage to the insured, exclusionary clauses are interpreted narrowly against the insurer." [Scottsdale Ins. Co. v. Van Nguyen](#), 158 Ariz. 476, 479, 763 P.2d 540, 543 (App. 1988).

Furthermore, “the policy may not be interpreted so as to defeat the reasonable expectations of the insured.” [Samsel v. Allstate Ins. Co.](#), 204 Ariz. 1, 4, 59 P.3d 281, 284 (2002). “Under this doctrine, a contract term is not enforced if one party has reason to believe that the other would not have assented to the contract if it had known of that term.” [First Am. Title Ins. Co. v. Action Acquisitions, LLC](#), 218 Ariz. 394, 400, 187 P.3d 1107, 1113 (2008); accord [Averett v. Farmers Ins. Co.](#), 177 Ariz. 531, 533, 869 P.2d 505, 507 (1994) (quoting [Gordinier](#), 154 Ariz. at 272, 742 P.2d at 283); [Darner](#), 140 Ariz. at 392, 682 P.2d at 397. “One of the basic principles which underlies [the doctrine] is simply that the language in the portion of the instrument that the customer is not ordinarily expected to read or understand ought not to be allowed to contradict the bargain made by the parties.” [Averett](#), 177 Ariz. at 533, 869 P.2d at 507 (quoting [State Farm Mut. Auto. Ins. Co. v. Bogart](#), 149 Ariz. 145, 151, 717 P.2d 449, 455 (1986), superseded by statute on other grounds as recognized in [Consolidated Enters., Inc. v. Schwindt](#), 172 Ariz. 35, 38, 833 P.2d 706, 709 (1992)).

\*4 The insured bears the burden of proving the applicability of the reasonable expectations doctrine at trial. [State Farm Fire & Cas. Ins. Co. v. Grabowski](#), 214 Ariz. 188, 190, 150 P.3d 275, 277 (App. 2007). The doctrine applies only if two predicate conditions are present. First, the insured’s “expectation of coverage must be objectively reasonable.” [Millar v. State Farm Fire and Cas. Co.](#), 167 Ariz. 93, 97, 804 P.2d 822, 826 (App. 1990). Second, the insurer “must have had a reason to believe that the [insured] would not have purchased the... policy if they had known that it included” the complained of provision. [Grabowski](#), 214 Ariz. at 193-94, 150 P.3d at 280-81. Provided both of these conditions are satisfied, “Arizona courts will not enforce even unambiguous boilerplate terms in standardized insurance contracts in a limited variety of situations.” [Gordinier](#), 154 Ariz. at 272, 742 P.2d at 283.

Finally, insurers expressly obligate themselves to defend their insureds against any claim of liability potentially covered by the policy. [Ariz. Prop. &](#)

[Cas. Ins. Guar. Fund v. Helme](#), 153 Ariz. 129, 137, 735 P.2d 451, 459 (1987); [United Servs. Auto. Ass’n v. Morris](#), 154 Ariz. 113, 118, 741 P.2d 246, 250 (1987). The duty to defend is triggered if the complaint “alleges facts which come within the coverage of the liability policy..., but if the alleged facts fail to bring the case within the policy coverage, the insurer is free of such obligation.” [Kepner v. Western Fire Ins. Co.](#), 109 Ariz. 329, 331, 509 P.2d 222, 224 (1973) (quoting C.T. Drechsler, Annotation, [Allegations in Third Person’s Action Against Insured as Determining Liability Insurer’s Duty to Defend](#), 50 A.L.R.2d 458 §3, at 464 (1956)). Indeed, an insurer rightfully refuses to defend only if the facts, including those outside the complaint, indisputably foreclose the possibility of coverage. See [Kepner](#), 109 Ariz. at 331, 509 P.2d at 224. “If the insurer refuses to defend and awaits the determination of its obligation in a subsequent proceeding, it acts at its peril, and if it guesses wrong it must bear the consequences of its breach of contract.” [Id.](#) at 332, 509 P.2d at 225.

### III. ANALYSIS

In its Complaint, Chang’s alleges that the Policy’s Insuring Clauses cover each assessment from the BAMS Letter. Specifically, Chang’s claims that Insuring Clause A covers ADC Fraud Recovery Assessment, Insuring Clause B covers the ADC Operational Reimbursement Assessment, and Insuring Clause D.2 covers the Case Management Fee. (Doc. 1-1.) Federal summarily argues that the BAMS Letter and the Assessments set forth therein do not fall within the coverage provided by any of the Policy’s Insuring Clauses. (Doc. 22 at 7.) Additionally, Federal contends that certain exclusions contained in the Policy bar coverage. ([Id.](#) at 11-16) The Court will analyze each Policy provision and exclusion in turn. Then the Court will turn to Chang’s final argument that coverage is proper under the reasonable expectation doctrine.

#### A. Insuring Clause A.

Insuring Clause A provides that, “[Federal] shall pay for **Loss**<sup>3</sup> on behalf of an **Insured** on account of any **Claim** first made against such **Insured**...for **Injury**.” (Doc. 8-1.) In relevant part, **Claim** means “a written request for monetary damages...against

an Insured for an **Injury**.” (*Id.*) Under the Policy, **Injury** is a broad term encompassing many types of injuries, including **Privacy Injury**. (*Id.*) **Privacy Injury** “means injury sustained or allegedly sustained by a **Person** because of actual or potential unauthorized access to such **Person’s Record**, or exceeding access to such **Person’s Record**.” (*Id.*) **Person** is a natural person or an organization. (*Id.*) Relevant to this discussion, **Record** includes “any information concerning a natural person that is defined as: (i) private personal information; (ii) personally identifiable information...pursuant to any federal, state...statute or regulation,...where such information is held by an **Insured Organization** or on the **Insured Organization’s** behalf by a **Third Party Service Provider**” or “an organization’s non-public information that is...in an **Insured’s** or **Third Party Service Provider’s** care, custody, or control.” (*Id.*) “**Third Party Service Provider** means an entity that performs the following services for, or on behalf of, an **Insured Organization** pursuant to a written agreement: (A) processing, holding or storing information; (B) providing data backup, data storage or data processing services.” (*Id.*)

\*5 Federal argues that Insuring Clause A is inapplicable because BAMS, itself, did not sustain a **Privacy Injury** because it was not its **Records** that were compromised during the data breach. (Doc. 22 at 8.) Federal therefore contends that BAMS is not even in a position to assert a valid **Privacy Injury Claim**.

Conversely, Chang’s argues that it was the Issuers who suffered a **Privacy Injury** because it was their **Records**, constituting private accounts and financial information, which were compromised in the data breach. (Doc. 36 at 6.) Chang’s argument is premised upon the idea that it is immaterial that this **Injury** first passed through BAMS before BAMS in turn charged Chang’s, because this was done pursuant to industry standards and Chang’s payment to BAMS was functionally equivalent to compensating the Issuers.<sup>4</sup> (See *Id.*) Basically, Chang’s argues that because a **Privacy Injury** exists and was levied against it, regardless of who suffered it, the **Injury** is covered under the Policy. (*Id.*)

Although the Court is expected to broadly interpret coverage clauses so as to provide maximum coverage for an insured, a plain reading of the policy leads the Court to the conclusion that Insuring Clause A does not provide coverage for the ADC Fraud Recovery Assessment. [Scottsdale Ins. Co.](#), 158 Ariz. at 479, 763 P.2d at 543. The Court agrees with Federal; BAMS did not sustain a **Privacy Injury** itself, and therefore cannot maintain a valid **Claim** for **Injury** against Chang’s. The definition of **Privacy Injury** requires an “actual or potential unauthorized access to *such Person’s Record*, or exceeding access to *such Person’s Record*.” (Doc. 8-1) (emphasis added). The usage of the word “such” means that only the **Person** whose **Record** is actually or potentially accessed without authorization suffers a **Privacy Injury**. Here, because the customers’ information that was the subject of the data breach was not part of BAMS’ **Record**, but rather the **Record** of the issuing banks, BAMS did not sustain a **Privacy Injury**.<sup>5</sup> Thus, BAMS did not make a valid **Claim** of the type covered under Insuring Clause A against Chang’s.

Contrary to Chang’s assertion, this interpretation is not a “pixel-level view” that “reduce[s] coverage to a mere sliver of what the plain language provides.” (Doc. 36 at 9.) Rather, this is the only result that can be derived from the Policy. It is also worth noting that Federal is not outright denying coverage in its entirety. Federal has reimbursed Chang’s nearly \$1.7 million for valid claims brought by injured customers and Issuers. As will be addressed more fully below, if Chang’s, who is a sophisticated party, wanted coverage for this Assessment, it could have bargained for that coverage. However, as is, coverage does not exist under the Policy for the ADC Fraud Recovery Assessment under Insuring Clause A.

#### **B. Insuring Clause B.**

Insuring Clause B provides that “[Federal] shall pay **Privacy Notification Expenses** incurred by an **Insured** resulting from [**Privacy**] **Injury**.” (Doc. 8-1.) The Policy defines **Privacy Notification Expenses** as “the reasonable and necessary cost[s] of notifying those **Persons** who may be directly affected by the potential or actual unauthorized



access of a **Record**, and changing such **Person's** account numbers, other identification numbers and security codes..." (*Id.*) Chang's alleges that the ADC Operational Reimbursement fee is a Privacy Notification Expense because it compensates Issuers for the cost of reissuing bankcards and new account numbers and security codes to Chang's customers. (Docs. 1-1, 36 at 8.)

\*6 In its motion, Federal uses similar argumentation it employed for Insuring Clause A. Federal contends that The ADC Operational Recovery fee was not personally incurred by Chang's, but rather was incurred by BAMS. (Doc. 22 at 10.) Also, Federal argues that the ADC Operational Recovery fee does not qualify as **Privacy Notification Expenses** because there is no evidence that the fee was used to "notify[ ] those **Persons** who may be directly affected by the potential or actual unauthorized access of a **Record**, and changing such **Person's** account numbers, other identification numbers and security codes." (*Id.*)

Chang's counters, stating that Federal's interpretation of "incur" is too narrow, as the Arizona Supreme Court held that an insured "incurs" an expense when the insured becomes liable for the expense, "even if the expenses in question were paid by or even required by law to be paid by other sources." (Doc. 36 at 8 (citing [Samsel](#), 204 Ariz. at 4-11, 59 P.3d at 284-91)).

The Court agrees with Chang's. Although the ADC Operational Reimbursement fee was originally incurred by BAMS, Chang's is liable for it pursuant to its MSA with BAMS.

In response to Federal's argument that there is no evidence that the ADC Operational Reimbursement fee was used to compensate Issuers for the costs of notifying about the security compromise and reissuing credit cards to Chang's customers, Chang's argues that MasterCard's Security Rules clearly state that the ADC Operational Reimbursement fee is used for that purpose. (Docs. 36 at 8, 24-1 at 84-88.) Federal does not direct the Court's attention to and the Court is unable to find any evidence in the record where the ADC Operational Reimbursement fee was used

for any other purpose. The evidence shows that MasterCard performed an investigation into the Chang's data breach and determined Assessments pursuant to the MasterCard Rules. MasterCard then furnished a Report to BAMS levying the ADC Operational Reimbursement fee against BAMS, which it paid and then imposed the Assessment upon Chang's. (Doc. 26-3.) The Court does not find this to be a question of fact more suitable for a jury, but rather can find as a matter of law that coverage exists for the ADC Operational Reimbursement under Insuring Clause B. However, this finding is subject to the Court's analysis of the Policy's exclusions discussed below.

### C. Insuring Clause D.2.

Under Insuring Clause D.2., "[Federal] shall pay:...**Extra Expenses** an **Insured** incurs during the **Period of Recovery of Services** due to the actual or potential impairment or denial of **Operations** resulting directly from **Fraudulent Access or Transmission**." (Doc. 8-1.) **Extra Expenses** include "reasonable expenses an **Insured** incurs in an attempt to continue **Operations** that are over and above the expenses such **Insured** would have normally incurred. **Extra Expenses** do not include any costs of updating, upgrading or remediation of an **Insured's System** that are not otherwise covered under [the] Policy." (*Id.*) In the context of **Extra Expenses**, **Period of Recovery of Services** "begins:...immediately after the actual or potential impairment or denial of **Operations** occurs; and will continue until the earlier of...the date **Operations** are restored,...to the condition that would have existed had there been no impairment or denial; or sixty (60) days after the date an **Insured's Services** are fully restored...to the level that would have existed had there been no impairment or denial." (*Id.*) **Operations** are an **Insured's** business activities, while **Services** are "computer time, data processing, or storage functions or other uses of an **Insured's System**." (*Id.*) **Fraudulent Access or Transmission** occurs when "a person has: fraudulently accessed an **Insured's System** without authorization; **Exceeded Authorized Access**; or launched a **Cyber-attack** into an **Insured's System**." (*Id.*)

\*7 Federal claims that Insuring Clause D.2. does not cover the Case Management Fee because Chang's has not submitted any evidence that the data breach caused "actual or potential impairment or denial" of business activities. (Doc. 22 at 11.) Chang's response states that the evidence clearly shows that its ability to operate was impaired because BAMS would have terminated the MSA and eliminated Chang's ability to process credit card transactions if it did not pay BAMS pursuant to the BAMS Letter. (Docs. 36 at 10, 23-2.) The MSA provides that Chang's is not permitted to use another servicer while contracting with BAMS for its services. (Doc. 23-2 at 3.) Furthermore, in her deposition, the approving underwriter for Federal, Leah Montgomery, states that she knew Chang's transacted much of its business through credit card payments and that Chang's would be adversely affected if it was unable to collect payment from credit card transactions. (Doc. 37-1 at 29.)

After reviewing the record, the Court agrees with Chang's. The evidence shows that Chang's experienced a **Fraudulent Access** during the data breach and that its ability to perform its regular business activities would be potentially impaired if it did not immediately pay the Case Management Fee imposed by BAMS. And, this Case Management Fee qualifies as an **Extra Expense** as contemplated by the Policy.

However, Federal argues that Chang's did not incur this **Loss** during the **Period of Recovery of Services** because it did not pay the Case Management Fee until April 15, 2015, nearly one year after it discovered the data breach. (Doc. 22 at 11.) Federal argues that because Chang's paid the Case Management Fee when it did, it falls outside the **Period of Recovery of Services**, which "begins:...immediately after the actual or potential impairment or denial of **Operations** occurs; and will continue until the earlier of...the date **Operations** are restored,...to the condition that would have existed had there been no impairment or denial; or sixty (60) days after the date an **Insured's Services** are fully restored...to the level that would have existed had there been no impairment or denial." (Doc. 8-1.) In response, Chang's contends that its business activities are still not fully restored

and that it continues to take steps to remedy the data breach; thus, the **Period of Recovery of Services** is ongoing. (Doc. 36 at 11.) Because this is an issue of fact, the Court is unable to resolve it on Summary Judgment. Accordingly, the Court cannot determine as a matter of law whether the Policy provides coverage for the Case Management Fee under Insuring Clause D.2.

#### **D. Exclusions D.3.b. and B.2. and Loss**

##### **Definition**

Federal also argues that Exclusions D.3.b. and B.2., as well as the definition of **Loss**, bar coverage for all of the Assessments. Exclusion D.3.b. provides, "With respect to all Insuring Clauses, [Federal] shall not be liable for any **Loss** on account of any **Claim**, or for any **Expense**...based upon, arising from or in consequence of any...liability assumed by any **Insured** under any contract or agreement." (Doc. 8-1.) Under Exclusion B.2., "With respect to Insuring Clauses B through H, [Federal] shall not be liable for...any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**." (Doc. 8-1.) Additionally, and along the same vein, **Loss** under Insuring Clause A does not include "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any **Insured**." (*Id.*) Functionally, these exclusions are the same in that they bar coverage for contractual obligations an insured assumes with a third-party outside of the Policy.

Federal contends that the assessments for which coverage is sought arise out of liability assumed by Chang's to BAMS, thus they are excluded from coverage. (Doc. 22 at 12.) Federal supports this argument by citing the MSA, wherein Chang's agreed that "[BAMS] may pass through to [Chang's] any fees assessed to [BAMS] by the Card Organizations, including but not limited to, new fees, fines, penalties and assessment[s]." (Doc. 23-1.) Federal also looks to the BAMS Letter where BAMS tells Chang's, "[i]n accordance with your Merchant Agreement you are obligated to reimburse [BAMS] for the...assessments." (Doc. 23-8.)

\*8 Chang's counters, offering a series of arguments why these exceptions are inapplicable in the present case. First, Chang's argues that such exclusions do not apply if "the insured is the one who is solely responsible for the injury," (citing [63 A.L.R.2d 1122](#) A.3d § 2[a] ), or, in other words, the exclusions do not apply to obligations the insured is responsible for absent any assumption of liability. (Doc. 36 at 12) (citing [Homeowners Mgmt. Enterp., Inc. v. Mid-Continent Cas. Co.](#), 294 Fed.Appx. 814 821 (5th Cir. 2008) and [Victoria's Secret Stores, Inc. v. Epstein Contracting, Inc.](#), 2002 WL 723215, \*4-5 (Ohio App. April 25, 2002)). Chang's argues that under the principal of equitable subrogation, it is compelled by "justice and good conscience," and not contractual liability, to compensate BAMS for the assessments. (Doc. 36 at 12) (citing [Sourcecorp., Inc. v. Norcutt](#), 227 Ariz. 463, 466-67, 258 P.3d 281, 284-85 (App. 2011)). Chang's argues this is an exception recognized in the law to contractual liability exclusions of this nature. (*Id.*) Additionally, Chang's argues that its "responsibility for the Loss is the functional equivalent of compensating for damages suffered by victims of Privacy Injury, regardless of the MSA." (Doc. 36 at 12.) Under this argument, Chang's states that it could be liable under a variety of theories, including: negligence or particular statutes, such as [A.R.S. § 44-7803](#), which places responsibility for fraudulent credit card transfers on merchants as opposed to credit card companies. (*Id.* at 12-13.) The Court is unconvinced by these arguments.

The Court finds that both Exclusions D.3.b. and B.2. as well as the definition of **Loss** bar coverage. In reaching this decision, the Court turned to cases analyzing commercial general liability insurance policies for guidance, because cybersecurity insurance policies are relatively new to the market but the fundamental principles are the same. Arizona courts, as well as those across the nation, hold that such contractual liability exclusions apply to "the assumption of another's liability, such as an agreement to indemnify or hold another harmless." [Desert Mountain Properties Ltd. P'ship v. Liberty Mut. Fire Ins. Co.](#), 225 Ariz. 194, 205, 236 P.3d 421, 432 (App. 2010), *aff'd*, 226 Ariz. 419, 250 P.3d 196 (2011) (citing [Smithway Motor Xpress, Inc. v. Liberty Mut. Ins. Co.](#), 484

[N.W.2d 192](#), 196 (Iowa 1992)); see also, [Gibbs M. Smith, Inc. v. U.S. Fid. & Guar. Co.](#), 949 P.2d 337, 341 (Utah 1997); [Lennar Corp. v. Great Am. Ins. Co.](#), 200 S.W.3d 651, 693 (Tex. App. 2006).

Chang's agreement with BAMS meets this criteria and thus triggers the exclusions. In no less than three places in the MSA does Chang's agree to reimburse or compensate BAMS for any "fees," "fines," "penalties," or "assessments" imposed on BAMS by the Associations, or, in other words, indemnify BAMS. (See Doc. 23-2 at 9, 18.) More specifically, Section 13.5 of the Addendum to the MSA reads: "[Chang's] agrees to pay [BAMS] any fines, fees, or penalties imposed on [BAMS] by any Associations, resulting from Chargebacks and any other fines, fees or penalties imposed by an Association with respect to acts or omissions of [Chang's]." (*Id.* at 9.) Furthermore, the Court is unable to find and Chang's does not direct the Court's attention to any evidence in the record indicating that Chang's would have been liable for these Assessments absent its agreement with BAMS. While such an exception to an exclusion of this nature may exist in the law, it is not applicable here. Accordingly, the Court must find that the above referenced exclusions bar coverage for all three Assessments claimed by Chang's.

In reaching this conclusion, the Court has followed the dictate that "exclusionary clauses are interpreted narrowly against the insurer." [Scottsdale Ins. Co.](#), 158 Ariz. at 479, 763 P.2d at 543. Yet, even while looking through this deferential lens, the Court is unable to reach an alternative conclusion. Simply put, these exclusions unequivocally bar coverage for the Assessments, including the ADC Operational Reimbursement that the Court said coverage existed for under Insuring Clause B.

#### **E. Reasonable Expectation Doctrine**

Finally, the Court turns to Chang's claim that in addition to coverage being proper under the Policy, coverage also exists pursuant to the reasonable expectation doctrine. (Doc. 36 at 14.) The doctrine applies only if two predicate conditions are present. First, the insured's "expectation of coverage must be objectively reasonable." [Millar](#), 167 Ariz. at 97,

804 P.2d at 826. Second, the insurer “must have had reason to believe that the [insured] would not have purchased the...policy if they had known that it included” the complained of provision. [Grabowski](#), 214 Ariz. at 193-94, 150 P.3d at 280-81. Chang’s bears the burden of proving the applicability of the reasonable expectation doctrine. *Id.*

\*9 Thus, the starting point for the reasonable expectations analysis is “to determine what expectations have been induced.” [Darner](#), 140 Ariz. at 390, 682 P.2d at 395. Chang’s states that the “dickered deal was for protection against losses resulting from [*sic*] a security compromise.” (Doc. 36 at 15.) By this, Chang’s means any and all fees and losses that flowed from the data breach, including the Assessments. Chang’s directs the Court’s attention to the deposition of Leah Montgomery, Federal’s approving underwriter who renewed the Policy that was in effect at the time of the data breach. There, the evidence shows that when Federal issued the Policy it understood the realities associated with processing credit card transactions. (See Doc. 37-1.) Federal knew that all of Chang’s credit card transactions were processed by a Servicer, such as BAMS, and the particular risks associated with credit card transactions. (*Id.* at 27, 85.) Federal also knew that Chang’s, a member of the hospitality industry with a high volume of annual credit card transactions, was a higher risk entity and therefore paid a significant annual premium of \$134,052.00. (*Id.* at 29, 75, 126.) Federal was also aware that issuers will calculate Fraud Recovery and Operational Reimbursement Assessments against merchants in an effort to recoup losses suffered by security breaches. (*Id.* at 87-91.) Furthermore, Chang’s also shows that Chubb markets the cyber security insurance policy as one that “address[es] the full breadth of risks associate with doing business in today’s technology-dependent world” and that the policy “Covers direct loss, legal liability, and consequential loss resulting from cyber security breaches.” (Doc. 37-7.)

Chang’s then argues that based on all of the above, it possessed the expectation that coverage existed under the Policy for the assessments. But this is a *non sequitur* conclusion unsupported by

the facts as presented. While Federal is aware of the realities of processing credit card transactions and that Chang’s could very well be liable for Assessments from credit card associations passed through to them by Servicers, this does not prove what Chang’s actual expectations were. Nowhere in the record is the Court able to find supporting evidence that during the underwriting process Chang’s expected that coverage would exist for Assessments following a hypothetical data breach. There is no evidence showing that Chang’s insurance agent, Kelly McCoy, asked Federal’s underwriter if such Assessments would be covered during their correspondence. (See Doc. 37-5.) The cybersecurity policy application and related underwriting files are similarly devoid of any supporting evidence. (See *Id.*; Doc. 37-6.)

Chang’s merely attempts to cobble together such an expectation after the fact, when in reality no expectation existed at the time it purchased the Policy. There is no evidence that Chang’s bargained for coverage for potential Assessments, which it certainly could have done. Chang’s and Federal are both sophisticated parties well versed in negotiating contractual claims, leading the Court to believe that they included in the Policy the terms they intended. See [Taylor v. State Farm Mut. Auto. Ins. Co.](#), 175 Ariz. 148, 158, 854 P.2d 1134, 1144 (1993); [Tucson Imaging Associates, LLC v. Nw. Hosp., LLC](#), No. 2 CA-CV 2006-0125, 2007 WL 5556997, at \*6 (Ariz. Ct. App. July 31, 2007). Because no expectation existed for this type of coverage, the Court is unable to find that Chang’s meets its burden of satisfying the first predicate condition, objective reasonableness, to invoke the reasonable expectation doctrine. This obviates the need to analyze this issue further. Therefore, the Court finds that coverage likewise does not exist under the reasonable expectation doctrine.

#### IV. CONCLUSION

Accordingly, based on the foregoing reasons, **IT IS HEREBY ORDERED GRANTING** Defendant Federal Insurance Company’s Motion for Summary Judgment. (Doc. 22.)

**IT IS FURTHER ORDERED DENYING** Plaintiff P.F. Chang’s China Bistro, Inc.’s Unopposed

Motion to Modify Case Schedule to Permit the Filing of an Amended Complaint (Doc. 44) as moot.

enter judgment in favor of Defendant and terminate the case.

Dated this 26th day of May, 2016.

**IT IS FURTHER ORDERED DISMISSING** Plaintiff P.F. Chang's China Bistro, Inc.'s complaint with prejudice. The Clerk of Court shall

**All Citations**

Not Reported in Fed. Supp., 2016 WL 3055111

Footnotes

- 1 The facts are undisputed unless indicated otherwise.
- 2 This total is separate from and does not include the \$1.7 million Federal has already paid Chang's under the Policy.
- 3 Terms in bold are defined in the Policy.
- 4 Chang's bolsters this argument by analogizing it to subrogation in other insurance contexts, which Federal misinterprets as the crux of Chang's argument. In reaching its decision, the Court gave appropriate weight to Chang's analogy, but does not believe this matter is governed by any subrogation legal rules.
- 5 BAMS also did not sustain any other type of **Injury** as defined under the Policy.

End of Document

© 2018 Thomson Reuters. No claim to original U.S. Government Works.





Michael Cardello III

*Partner*

mcardello@moritthock.com

Martindale-Hubbell®



## MICHAEL CARDELLO III

### Practice Areas

Commercial Litigation  
Alternative Dispute Resolution  
Bankruptcy

Michael Cardello III has been a partner with the firm since 2006. He currently Co-Chairs the firm's Litigation practice group and serves on the firm's Management Committee. Mr. Cardello concentrates his practice in business and commercial litigation. Prior to joining the firm in 1997, he served as a Law Clerk to the Honorable Arthur D. Spatt, United States District Court for the Eastern District of New York.

Mr. Cardello represents large and small businesses, financial institutions and individuals in Federal and State Courts in complex commercial matters. He has a wide-range of experience that includes trials and appellate work in the areas of corporate disputes, shareholder derivative actions, dissolutions, construction disputes, equipment and vehicle leasing disputes and other complex commercial and business disputes.

Mr. Cardello also serves as a Court-Appointed Discovery Referee and Special Referee by various courts to oversee all aspects of the discovery process in complex commercial cases. From 2005 through 2008, Mr. Cardello oversaw all aspects of discovery in Delta Financial Corp. v. Morrison, in which he rendered many written decision related to discovery, e-discovery and privilege issues and presided over sixty-five depositions. From 2009 through 2015, Mr. Cardello served as Special Referee in a very large multi-party construction defect case captioned Archstone v. Tocci Building Corporation of New Jersey. During his appointment, Mr. Cardello issued numerous decisions regarding complex e-discovery issues as well as issuing decisions on other non-dispositive motions. From 2012 to 2016, Mr. Cardello served as the Special Referee in the related insurance coverage action to the Archstone construction defect case, captioned QBE Insurance Corporation v. Adjo Contracting Corporation. During his tenure, Mr. Cardello issued numerous decisions and rulings in order to prepare the case for trial. Mr. Cardello was also involved in the settlement process, which lead to a resolution.

From 2013 to 2016, Mr. Cardello served as the Special Referee to oversee the dissolution of a law firm and the wind up of its affairs. During his appointment, Mr. Cardello dealt with many legal issues and was successful in separating the law firm into two firms. On consent of the parties, he has presided over a trial on one unresolved issue related to the wind up which resulted in a settlement. He is currently appointed to a number of cases as Discovery Referee and Special Referee by Justices of the Supreme Court for the State of New York.

Mr. Cardello is also approved by the Officer of Court Administration in the State of New York to serve as a Receiver and has been appointed by the Court as Receiver to oversee the dissolution and wind up of the affairs of businesses and for the collection of rents for commercial properties. Mr. Cardello currently serves as a Court Appointed Receiver for a 250,000 square foot office building that is the subject of a commercial foreclosure. He also mediates complex commercial litigation matters for cases pending in the Commercial Division of the Supreme Court of the State of New York.

Mr. Cardello is the Chair of the Federal Courts Committee and former Chair of the Commercial Litigation Committee of the Nassau County Bar Association. He is also a member of its Alternative Dispute Resolution and Judiciary Committees. He is also the District Leader for the 10<sup>th</sup> Judicial District for the Commercial and Federal Section of the NYSBA. In addition, he is a participant at the Sedona Conference and also frequently lectures on mediation, discovery, trial practice, equipment and vehicle leasing issues and e-discovery.

### **Education**

Hofstra University, J.D.

*Associate Editor, Hofstra Law Review*

Hofstra University, M.B.A. (Finance)

Hofstra University, B.B.A. (Marketing)

### **Admissions**

Mr. Cardello is admitted to practice law in New York. He is also admitted to practice in the Eastern and Southern Districts of New York and the United States Court of Appeals for the Second Circuit.

### **Affiliations**

Mr. Cardello serves on the EDNY Litigation Advisory Committee, and serves as Chair of the Nassau County Bar Association's Federal Courts Committee, as well as on its WE CARE Fund Advisory Board. In addition, he also serves as Chair of the Board of Directors for the Metro New York/Connecticut Chapter of the National Vehicle Leasing Association. Mr. Cardello is also a member of the Catholic Lawyers Guild of Nassau County and serves as its Secretary. Mr. Cardello is also the current President of the Theodore Roosevelt American Inn of Court. He serves as a fellow and on the Board of the Academy of Court-Appointed Masters, as well as on the Board of Directors for Long Island Counsel for Alcohol and Drug Dependence.

### **Recognitions**

2017-New York Super Lawyers®

2016-New York Super Lawyers®



## CONTACT

**Juan Luis García**  
Associate

**Long Island**  
50 Jericho Quadrangle  
Suite 300  
Jericho, NY 11753-2728  
Phone: 516-832-7550  
Fax: 855-718-2103  
jgarcia@nixonpeabody.com

## SERVICES

Litigation  
Complex Commercial Litigation  
Insurance Litigation  
Insurance  
Products: Class Action, Trade &  
Industry Representation  
Consumer Products  
Pharmaceutical & Medical Device  
Litigation  
Appellate  
Arbitration  
Aviation Product Liability

## EDUCATION

Columbia University School of  
Law, J.D., *Human Rights Law*  
*Review*  
University of Kansas, B.A., *summa*  
*cum laude*, Phi Beta Kappa

## ADMISSIONS

New York

## JUAN LUIS GARCÍA

Juan Luis is a trial and appellate attorney who represents businesses in the manufacturing, insurance, health care, life sciences, medical device and other industries in disputes in federal and state courts and arbitrations.

---

### What do you focus on?

#### Complex Commercial Disputes

I have broad experience defending and prosecuting complex commercial disputes, often between businesses or involving investors and executives, in connection with often high-stakes issues and significant financial or reputational concerns for our clients. My range of experience includes civil RICO and fraud claims, breaches of stock purchase and other acquisition agreements, franchising issues, trade secret misappropriation, intellectual property, misleading business practices, trade libel, breaches of fiduciary duties, and indemnity issues. I also have experience counseling and defending businesses in connection with their employment practices. I develop and apply timely, tailored strategies for each case, from pre-suit investigation, to fact and expert discovery, to trial and appeals.

#### Insurance Coverage

I represent clients in the insurance industry handling diverse coverage issues—including interpretations of provisions that may lack prior legal construction, computer fraud and cyber risk coverage, issues relating to tiers of coverage, and allocation issues among insurers. Having litigated a wide variety of complex commercial disputes, I can effectively scrutinize and analyze the liability claims underlying difficult coverage disputes. I enjoy collaborating with our clients' in-house legal teams to align our strategies with our clients' business and risk-management objectives.

#### Products Defense and Regulatory Counseling

I have worked with large manufacturers in a spectrum of sectors, including the heating and air conditioning, trucking, aviation, medical devices and children's products fields, to vigorously defend their products and provide counseling and opinions regarding regulatory and litigation risks. I work closely with my clients' quality control, design and legal or business teams to develop a deep understanding



U.S. District Court, Eastern  
District of New York

U.S. District Court, Northern  
District of New York

U.S. District Court, Southern  
District of New York

## **LANGUAGES**

French

Spanish

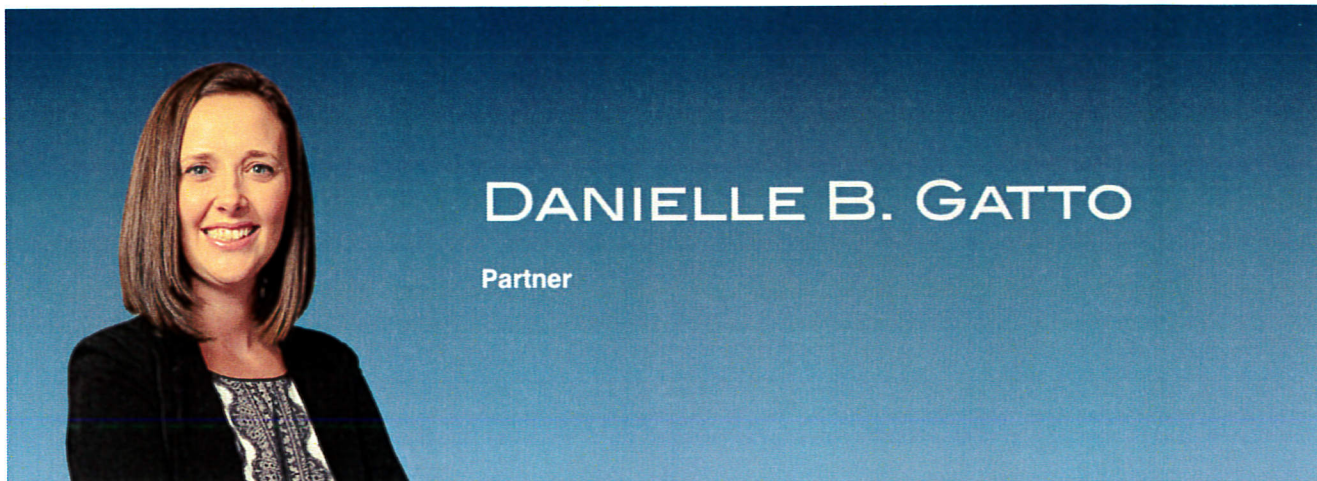
of the products at issue and prepare a defense that matches my clients' strategic objectives for all phases of litigation.

My regulatory experience spans counseling with regard to regulations enforced by the Food and Drug Administration, the Federal Trade Commission, and the Consumer Products Safety Commission. I also counsel various manufacturers and technology startups with regard to documentation, advertising, warranty and privacy issues.

---

## **Publications and Presentations**

- "Risky business: Integrating privacy and security from the start," LaunchPad Huntington, August 21, 2014 (co-presenter)
- "Regulatory Risks and Opportunities for New Technologies in Smart Sensors and Wearables," *Legal Diagnostics Blog*, June 11, 2014
- "The Consumer Product Safety Commission and Consumer Product Safety," NYC Bar Association, May 2014 (co-presenter)



## DANIELLE B. GATTO

Partner

**Email:** [dgatto@forchellilaw.com](mailto:dgatto@forchellilaw.com)

**Phone:** (516) 248-1700

**Fax:** (866) 522-7811

Danielle B. Gatto is a partner in the litigation group, concentrating her practice in the areas of commercial litigation, real property actions, zoning matters, and employment litigation—as well as assisting with complex tax certiorari matters and defending First Amendment actions. Ms. Gatto also has extensive experience with adverse possession and prescriptive easement claims. Ms. Gatto has successfully argued before the Appellate Division, as well as in state and in federal court proceedings. She also has significant experience with motion and trial practice in state and federal courts, representing individuals, corporations, and municipalities.

While at Hofstra University School of Law, she was the symposium editor of the Hofstra Labor & Employment Law Journal and a member of the Moot Court Association. She also traveled to New Orleans, Louisiana over her spring breaks in order to provide free legal service to Hurricane Katrina victims. Furthermore, while at Hofstra, she received a Merit Scholarship and was awarded a Bronze Pro Bono Program Certificate. While earning her degree, Ms. Gatto worked as a law clerk with the Firm. Prior to working for the Firm, Ms. Gatto had a judicial internship with Justice Stephen A. Bucaria of Nassau County Supreme Court and a legal internship at the United States Attorney's Office for the Eastern District of New York.

Ms. Gatto has published the following: "Limiting the Unrestricted Motion in Limine," in the New York Law Journal, which she co-authored; "The Improper Use of Motions in Limine," in the Nassau Lawyer, also co-authored; and authored "New Legislation to Promote a 'Healthy' Workplace," in the Hofstra Labor and Employment Law Journal blog.

She has received the Long Island Young Professionals Award (2013), was named an Outstanding Woman in the Law (2016), and has been named a *New York SuperLawyers Rising Star* in Business Litigation from 2015 to 2017.

### PRACTICE AREAS

- [Employment & Labor \(/practice-groups/employment-labor/\)](#)
- [Litigation \(/practice-groups/litigation/\)](#)

### EDUCATION

- Hofstra University School of Law, 2009
- Tulane University, B.A., 2006

### ADMISSIONS

- New York State Bar
- United States District Court for the Eastern and Southern Districts of New York

### PROFESSIONAL AFFILIATIONS AND ACCOMPLISHMENTS

- Nassau County Bar Association (Commercial Litigation Committee)
- Theodore Roosevelt American Inn of Court



Steven S. Rubin  
*Partner (CIPP/US)*  
srubin@moritthock.com

## STEVEN S. RUBIN

### Practice Areas

Trademarks, Patents & Other Intellectual Property  
Cybersecurity  
Litigation

With a degree in Electrical Engineering, Steve Rubin is a Partner with the firm where he Chairs its Patent Practice Group and Co-Chairs its Cybersecurity Practice Group.

Mr. Rubin has over 20 years of experience in consulting clients on patent related matters. He advises clients throughout all phases of a patent's life from conception by an inventor to enforcement. He drafts and prosecutes patent applications and has managed large international patent portfolios. In addition, Mr. Rubin also identifies potential patent infringement assertions and potential cross-licensing opportunities and provides infringement opinions as needed. He handles Inter Partes Reviews (IPRs), Covered Business Methods Patent Reviews (CBMs), and Post-Grant Reviews (PGRs) before the Patent Trial and Appeal Board (PTAB). He represents clients in patent enforcement and litigation matters domestically and internationally and reviews patent portfolios and pending patent litigations in relation to corporate mergers, acquisitions and investments. He also represents companies of all sizes from start-ups to multi-national corporations.

In the cybersecurity/privacy space, Mr. Rubin relies on his technology background in counseling clients and creating written information security policies (WISPs). The WISP may be used by companies to mitigate the risk of, and potentially limit exposure from, a data breach. In generating a WISP, Mr. Rubin may serve the role of an external Chief Information Security Officer ("CISO") as is required under 23 NYCRR § 500 *et seq.* He also counsels clients in privacy issues such as advising on GDPR (General Data Protection Regulation) compliance. Mr. Rubin serves as part of a multi-disciplinary team that can be called into action when a company is sued for actions associated with a data breach.

Mr. Rubin focuses his practice on technology relating to electronics and computer science and has worked in diverse fields such as software; multi-core architecture; augmented reality; 3-D printing; optical communication; information processing; image processing; security systems; video conferencing; network based technologies, including cloud computing; mobile applications; search engines; military defense systems; physics; material science; encryption; chemical engineering; nanotechnology; medical devices; microlithography; RF-ID; fabrication and production of semiconductor devices; computer and network

architecture and monitoring; circuits; coding/decoding, processing and transmission of signals; antennas; cell phone and pager technology; printer and display technology including LCD control; transmission, compression, synchronization, processing, and display of television signals; optical communications and lens technologies; mechanical devices; and lighting circuitry.

As a recognized leader in his field, Mr. Rubin speaks and publishes extensively on various issues and topics pertaining to patent law and cybersecurity law. He has been quoted in *IP Law & Business*, *Forbes Magazine*, *Information Week*, *World Intellectual Property Law Review*, *macnewsworld.com*, *ecommercetimes.com*, *computerworld.com*, *TechNewsWorld*, *Linuxinsider*, *EE Times*, *IPLaw360.com*, *Information Display Magazine*, *Newsday* and *Long Island Business News*, and in December 2012, he appeared as a legal analyst on PBS's Nightly Business Report (NBR) "Profiting from Patents".

In addition to his legal career, Mr. Rubin mentors law students at Hofstra University School of Law. He has also taught intellectual property law at Stony Brook University, as well as patent law at Brooklyn Law School, Fordham University School of Law, Stony Brook University and Farmingdale State College.

### **Education**

Hofstra University, J.D. 1997

*Articles Editor, Hofstra Law & Policy Symposium*

New York Institute of Technology, B.S. (Electrical Engineering, *magna cum laude*) 1994

### **Admissions**

Mr. Rubin is admitted to practice in New York and New Jersey. He is also admitted before the United States Patent and Trademark Office, as well as before the U.S. District Courts for the Eastern and Southern Districts of New York.

### **Affiliations**

Mr. Rubin is currently serving as the Chair of the IP Transactions and Licensing Committee in the American Bar Association Section of Intellectual Property Law (ABA-IPL) and is active in other committees in ABA-IPL. He also serves on the industry advisory board for New York Institute of Technology. He is a member, *senior grade*, of IEEE (Institute of Electrical and Electronics Engineers) and a corresponding member of the IEEE-USA Intellectual Property Law Committee. He is the past Chairman of the IEEE Long Island Section Power & Energy and Industrial Applications Joint Societies Chapter and currently serves as the Legal Affairs Section Officer for the Long Island Chapter. Mr. Rubin is also a member of Eta Kappa Nu (the electrical and computer engineering honor society) and was a featured professional in its autumn 2007 publication of *The Bridge*.



## **Certifications**

Certified Information Privacy Professionals (CIPP/US).

## **Awards**

In December 2009, Mr. Rubin received a "Power & Energy Society Chapter Outstanding Engineer Award" for his contributions to the engineering profession and for his leadership in the formation of its Long Island Chapter.

## **Speaking Engagements**

Presenter, *Request for Production Number 23: Produce all documents relating to any WISP that existed prior to the Data Breach - How To Limit Potential Legal Liability in the Event of a Data Breach*, Business Fundamentals Bootcamp, September 28, 2017.

Presenter, *Managing Cybersecurity Due Diligence in Technology M&A Transactions*, American Bar Association, Webinar, September 12, 2017.

Featured Speaker, *How To Limit Your Potential Legal Exposure From A Data Breach*, Geneva Group International's European Regional Conference, Brussels, Belgium, May 11-14, 2017.

Featured Speaker, *Technology Transfer Days Meetup Event Series – Legal and Collaborative Learning Session*, Technology Transfer Days Meetup Event Series, April 25, 2017.

Presenter, *From Technology to Taxation: The Interaction Between Intellectual Property Law and Transfer Pricing Rules Applicable to Intangibles Transfers Between Controlled Parties*, American Bar Association, January 2017.

Presenter, *Patent Exhaustion*, Lawline.com Webinar, December 13, 2016.

Presenter, *An Overview of the Various Protections Provided by Intellectual Property Laws*, Lawline.com Webinar, December 13, 2016.

Presenter, *Design Patents, Copyrights and User Interfaces*, Lawline.com Webinar, December 13, 2016.

Presenter, *Protecting Your Company's IP Assets: A Presentation on Copyrights, Trademarks, Trade Secrets, Utility Patents, Design Patents and Cybersecurity*, September 27, 2016.

Presenter, *Completing Invention Disclosure Forms To Create Licensable Property*, April 2016.

Presenter, *Protecting Your Company and Its Employees Against Data Breach Liability, Fraud and Employee Benefit Plan Failures*, November 2015.

Presenter, *Patent Exhaustion: Understanding the Issues in Lexmark v. Impression Products*, September/October 2015.

Panelist, *The Cyber Security Breach Notification Team*, ASBDC Cyber Security Conference 2015, sponsored by Ramapo College, August 2015.

Presenter, *Introduction to Intellectual Property*, May 2015.

Presenter, *Preparing for Data Breach Response and Litigation*, May 2015.

Presenter, *United States Patent Law Spring 2015 Update*, May 2015.

Presenter, *Cybersecurity and Data Breaches: Can I Trust You With My Financial Data?*, April 2015.

Presenter, *Request for Production Number 23: Produce all documents relating to any WISP that existed prior to the Data Breach - How To Limit Potential Legal Liability in the Event of a Data Breach*, LISTNET, March 2015.

Presenter, *United States Patent Law Winter 2015 Update*, March 2015.

Presenter, *Cyberattacks and Data Breaches: Your Businesses' Largest Risk: Learn How To Protect Your Business*, Trade Nassau Cybersecurity Conference, November 2014.

Presenter, *Cybersecurity, Restrictive Covenants & Intellectual Property 101*, October 2014.

Presenter, *Practical Approaches To Protect Your Intellectual Property & Limit Data Breach Liability*, Alcott HR & M&T Bank Cybersecurity Seminar, October 2014.

Presenter, *Patent Law Update Fall 2014*, September 2014.

Presenter, *Practical Approaches To Limit Data Breach Liability*, NYIT 2014 Cybersecurity Conference, September 2014.

Presenter, *Patent Eligibility: Is Your Invention So Abstract The Law Doesn't Care If It's Obvious?*, September 2013.

Presenter, *You May Not Be 007, but Your IP Is Worth Protecting As If It Was A MI6 Database*, March 2013.

Presenter, *Understanding the Implications of America Invents Act*, March 2011.

Presenter, *Protecting and Securing IP and Computing Inventions*, New York Institute of Technology Cyber Security Conference, September 2010.

Presenter, *Securing and Protecting Your Intellectual Property, What Can Small Companies Learn From Their Larger Rivals?* Long Island Forum for Technology Information Technology (LIFT-IT) Security Committee, February 2009.

Presenter, *Acquiring Patent/Intellectual Property Protection For Electronic Circuits and Systems*, Institute of Electrical and Electronics Engineers (IEEE) New York Section Event-co-sponsored by the Consultants Network and the Professional Activities Committee for Engineers (PACE), September 2008.

Presenter, *General Patent Protection of Intellectual Property as Applied to Circuit and Systems*, Circuits and Systems Society - Long Island Section of the Institute of Electrical and Electronics Engineers (IEEE), June 2008.

Presenter, *Understanding the Implications of the Patent Reform Act of 2007*, Institute of Electrical and Electronics Engineers (IEEE) Long Island Systems, Applications, and Technology Conference, May 2008.

Presenter, *Supreme Changes in Patent Law*, Computer Society-Long Island Section of the Institute of Electrical and Electronics Engineers (IEEE), July & October 2007.

Panelist, *Patent Litigation After eBay*, Teleseminar sponsored by IPLaw360.com, September 2006.

### **Published Articles**

Quoted in "Equifax Hack Teaches Hard Lessons About Data Regulation and Incident Response," *www.Law.com*, September 11, 2017.

Quoted in "Equifax Breach Reveals Gaping Flaw in Regulation Over the Storage of Data," *The New York Times*, September 9, 2017.

Quoted in "Massive Equifax Cyberattack May Push Congress on Breach Notice Law," *www.bna.com*, September 8, 2017.

Quoted in "Seriously, Equifax? This Is A Breach No One Should Get Away With," *The New York Times*, September 8, 2017.

Quoted in "Equifax Cyberattack May Push Congress Breach Notice," *Bloomberg BNA*, September 8, 2017.

Quoted in "Disaster Recovery vs. Security Recovery Plans: Why You Need Separate Strategies," *www.csoonline.com*, August 24, 2017.



Quoted in "LI cybersecurity experts on hack attack: Be prepared," *www.newsday.com*, May 16, 2017.

Quoted in "Global Cyberattack Wave Ebbs; LI May Have Missed The Brunt," *www.newsday.com*, May 15, 2017.

"A Restricted Sale Outside The United States Could Exhaust Your U.S. Patent Rights," *MH&H Alert May 2017*.

"Shop Until You Drop, Or Until The Supreme Court Says To Stop, The Supreme Court Limits 'Venue Shopping' For Patent Cases," *MH&H Alert May 2017*.

The Internet Of Things: Marrying Cybersecurity With Product Liability Litigation," *GGI – Litigation & Dispute Resolution Newsletter*, Spring 2017.

"Encryption: Taking a Step Towards Limiting Legal Liability For a Data Breach", *MH&H Alert*, April 2017.

"SCOTUS Laches Ruling Won't Have 'Monumental' Impact, Say Lawyers", *World Intellectual Property Review*, March 2017.

"Is Your Design Worth \$400 Million Dollars?", *MH&H Alert*, December 2016.

Quoted in "Record Breach," <https://news.vice.com>, " December 23, 2016.

Quoted in "IT Professionals Hold Little Back in Reaction to Yahoo Breach, *www.eweek.com*, December 16, 2016.

Quoted in "Workers Are Key To Preventing Cyber Attacks," *www.IdahoBusinessReview.com*, November 14, 2016.

"When Coffee Makers Attack", *Computerworld.com*, October 27, 2016.

"Seize That Flash Drive! The Defend Trade Secrets Act Necessitates Immediate Action By Employers, Expands The Scope Of Trade Secrets And Provides For Seizure Remedies", *MH&H Alert*, August 2016.

"U.S. and EU Tech Companies at Sea with End of Data Safe Harbor", *Computerworld.com*, July 26, 2016.

"International Cybersecurity Compliance Concerns," *The Corporate Counselor, ALM*, Vol. 31, No. 4, July 2016.

"Recovery Teams & Crisis Management", *A Business Owner's Practical Guide to Cybercrime & Business Continuity*, October 2015.

"Meeting Your Cybersecurity Obligations", *NYSBA* Vol. 33, No. 2, Fall 2015.

"Counsel's Capacity to Control Cybersecurity Costs, *New York Law Journal*, August 12, 2015.

"Patent Office Issues Guidelines Defining a Path For Subject Matter Eligibility", *MH&H Alert*, August 2015.

"*Teva v. Sandoz*: Identifying Your Person of Ordinary Skill in the Art; Proceed with Care, *MH&H Alert*, February 2015.

"Cyber Wars and the Legal Lessons from the Sony Hack", *Livescience*, December 27, 2014.

"Sony Facing 2 Suits By Ex-Workers Over Data Breach", *Associated Press Online*, December 16, 2014.

"Will Your Patented Software Survive An Abstract Idea Hearing?" *Institute of Electrical and Electronics Engineers (IEEE-USA), Today's Engineer*, July 15, 2014.

"Telsa Can Keep Its Patents", *Livescience*, July 15, 2014.

"Patented Software, the Supreme Court & Abstract Idea Hearings" *EE Times*, July 10, 2014.

"Common Sense Tips To Protect Your Company From A Data Breach", *MH&H Alert*, July 2014.

"Will Your Patented Software Survive An Abstract Idea Hearing?" *MH&H Alert*, June 2014.

"Taking Steps To Cybersecurity", *Newsday*, May 12, 2014.

"I Think Someone Is Stealing Our Data. What Should We Do?" *MH&H Alert*, March 2014.

"Targeting Data Breaches", *Long Island Business News*, February 14, 2014.

"Legal Standards Proposed For Cybersecurity-Is Your Company In Compliance?" *MH&H Alert*, January 2014.

"Indecision By Federal Circuit Provides Clear Guidance (Software Is Patentable Except When It's Not)", *MH&H Alert*, May 2013.

"Laboring Through The America Invents Act", *MH&H Alert*, May 2012.

"Do NOT Publish That Article (If You Care About Patent Rights In The United States)", *Institute of Electrical and Electronics Engineers (IEEE-USA) Today's Engineer Online*, December 2011.

"New Patent Law Might Invalidate Business Method Patents Altogether" *BetaBeat.com*, September 2011.

"Here's An Idea, Why Not Patent It? A Brief Summary Of The Issues and Complexities Of *Bilski v. Doll*", *Institute of Electrical and Electronics Engineers (IEEE-USA) Today's Engineer Online*, September 2009.

"Can I Patent That? Obtaining and Maintaining Patent Protection On Circuits and Systems In 2008", *Institute of Electrical and Electronics Engineers (IEEE) Circuits and Systems Magazine*, December 2008.

"Understanding The Implications Of The Patent Reform Act of 2007", *Institute of Electrical and Electronics Engineers (IEEE) Systems, Applications and Technology Conference Publication (pages 1-5)*, May 2008.

"Supreme Makeover: Software Patent Edition", *Software Development Times*, November 1, 2007.

"Defending the Patent Troll: Why These Allegedly Nefarious Companies Are Actually Beneficial To Innovation", *The Journal of Private Equity*, Fall 2007.

"KSR v. Teleflex: The Patent Case That Will Obviously Affect Your Business", *Computerworld.com*, April 30, 2007.

"Hooray For The Patent Troll!" *Institute of Electrical and Electronics Engineers (IEEE) Spectrum Online*, March 2007.

"How To Groom Patents: When Changes Are Needed, Reissue, Re-Examination and Certificate Of Correction Come To The Rescue", *New York Law Journal*, February 20, 2007.

"eBay v. MerceExchange: Did The Supreme Court Concurrence Crush Claimants Who Chose Not To Commercialize?" *IPLaw360.com*, June 20, 2006.

"Microsoft-Eolas Dispute Highlights Patent Reexamination", *IP Litigation Quarterly*, December 2003.

## Steve Treglia

Steve was a prosecutor in New York between 1980 and 2010, the last 14 years of which he spent as founder and head of the Cybercrime Unit at the Nassau County DA's Office, a Unit which utilized its own in-house forensic and undercover online investigators. Prior to investigating cybercrime, he had been an organized crime prosecutor for 10 years in the Queens and Nassau DA's Offices.

Upon retiring from law enforcement in 2010, he joined Absolute Software Corporation, headquartered in Vancouver, BC. Its software tracks stolen mobile devices by Absolute's investigative staff (all former law enforcement). Steve oversaw the investigative staff to ensure they conducted their investigations lawfully and in compliance with varying privacy requirements from one geographical jurisdiction to another. During his tenure with Absolute, the investigative staff recovered over 40,000 stolen mobile devices.

Since Absolute's customers included a large number of healthcare entities, Steve assumed the responsibility of acquiring HIPAA training and became the HIPAA Compliance Officer for the Investigations Division. He secured his HealthCare Information Security and Privacy Practitioner certification from the International Information System Security Certification Consortium in 2015.

In January of 2018, Steve joined Cordium in New York City, a GRC Consulting Company. He holds the title of Cyber & Information Security Consultant, and is currently specializing in HIPAA and EU's General Data Privacy Regulation compliance with Cordium's clients.

Over the last 20 years, he has become a nationwide lecturer and writer on a number of cybercrime and cybersecurity related issues. He has written a regular technology law column in the New York Law Journal since 2002, and numerous others of his technology articles have been published in various business, legal and technical journals. He has lectured on cybercrime and privacy issues before the FBI, DEA, RSA, National Association of Attorneys General, National District Attorney Association, High Technology Crime Investigation Association, New York State Cybersecurity Conference, and New York Prosecutors' Training Institute, to name just a few organizations. Since 2004, he has helped train forensic investigators with the FBI's Computer Analysis and Response Team by playing the roles of prosecutor and defense attorney in Moot Court Training.



## Hon. Ira B. Warshawsky

Of Counsel

990 Stewart Avenue  
Garden City, New York 11530  
(516) 741-6565  
iwarshawsky@msek.com

### Practice Areas

Litigation & Dispute Resolution  
Professional Responsibility  
Alternative Dispute Resolution

### Education

Brooklyn Law School  
J.D., 1969

Rutgers University  
B.A., 1966

### Memberships

American Bar Association  
New York State Bar Association  
New York Bar Foundation, Fellow  
Nassau County Bar Association,  
Former Director; Community  
Relations & Public Education Committee, and  
Strategic Planning Committee, former Chairs  
Nassau County District Court Judges'  
Association, Past President  
Assistant District Attorneys Association  
of Nassau County, Past President  
Jewish Lawyers Association  
Nassau Academy of Law, Former Dean  
Theodore Roosevelt American Inn of Court,  
Member and Past President  
American College of Business Court Judges,  
Founding Member and Past President  
Special Masters of Commercial Division,  
New York County

### Admissions

New York State

Justice Ira B. Warshawsky, ret. is Of Counsel in the Litigation and Alternative Dispute Resolution practices at Meyer, Suozzi, English & Klein, P.C. in Garden City, Long Island, N.Y. Since joining the firm, the judge has handled mediations with a concentration in construction cases, along with litigation matters. The Judge serves not only as an advocate, representing clients in commercial litigation, but also as a mediator, arbitrator, litigator, private judge and referee, especially in the area of business disputes and the resolution of electronic discovery (E-Discovery) issues. The Judge is also a member of NAM's arbitration and mediation panels. Judge Warshawsky has been a distinguished member of the New York judiciary for the past 25 years. Immediately prior to joining Meyer Suozzi, he served as a Supreme Court Justice in one of the State's leading trial parts -- the Commercial Division -- where he presided over all manner of business claims and disputes, including business valuation proceedings, corporate and partnership disputes, class actions and complex commercial cases.

Judge Warshawsky started his career in public service as a Legal Aid attorney in 1970 when he was Assistant Chief of the Family Court branch in Queens County. He served as a Nassau County Assistant District Attorney in the District and County Court trial bureaus from 1972 to 1974. Following these four years of prosecution and defense work he became a law secretary, serving judges of the New York State Court of Claims and County Court of Nassau County. In 1987 he was elected to the District Court and served there until 1997. In 1997 he was elected to the Supreme Court of the State of New York where he has presided in a Dedicated Matrimonial Part, a Differentiated Case Management Part and sat in one of the county's three Dedicated Commercial Parts until 2011.

Judge Warshawsky has been active in numerous legal, educational and charitable organizations during his career. The Judge recently served as an expert in New York Law in the Grand Court of the Cayman Islands. He has also served as a lecturer in various areas of commercial, civil and criminal law, most recently in the area of e-discovery and its ethical problems. He frequently lectures for the National Institute of Trial Advocacy (NITA) at Hofstra and Widener Law Schools. The Judge currently serves as a contributing editor of the *Benchbook for Trial Judges* published by the Supreme Court Justices Association of the State of New York. He has served as a member of the Office of Court Administration's Civil Curriculum Committee. In 2010, while still on the bench, he was named the official representative of the New York State Unified Court System to The Sedona Conference®, a leading organization

## Hon. Ira B. Warshawsky

credited with developing rules and concepts which address electronically stored information in litigation. The judge is currently a member of the Advisory Board of The Sedona Conference.

As a judge in the Commercial Division of the Supreme Court, he authored several informative decisions dealing with the discoverability and cost of producing electronic materials as well as determining “fair value” in corporate dissolution matters. He has presented numerous seminars on electronic discovery to practicing lawyers through the ABA, the NYSBA, the Nassau Bar Association and private corporate law forums.

In 1996 Judge Warshawsky was the recipient of EAC's Humanitarian of the Year Award, in 1997 he received the Nassau County Bar Association President's Award, in 2000 he received the Former Assistant District Attorneys Association's Frank A. Gulotta Criminal Justice Award and in 2004, the Nassau Bar Association's Director's Award. He is also past president of the Men of Reform Judaism, the men's arm of the Union of Reform Judaism, the parent body of the Reform movement of Judaism. In 2015, Judge Warshawsky was voted as one of the top 10 Arbitrators in a *New York Law Journal* reader's poll. In 2016, he was named an “ADR Champion” by the *National Law Journal*.