What goes in cyberspace stays in cyberspace

(Making Cybersecurity a Surety)

The program will center on the tension between technology that makes our lives and work easier and able to be done remotely with the need and obligation to keep information secure and confidential. The program will attempt to educate on the various issues surrounding the use of technology and how best to secure data and keep client's information confidential. The program will explore the need to be vigilant and aware of the ethical concerns about using devices for work and not maintaining proper security measures. A discussion of the model rules such as 1.1 and 1.6 would be applicable to this topic. The program will also attempt to juxtapose the problems of hacking versus the more simple breaches such as failure to secure devices. There will be skits that develop these problems in order to highlight what not to do and to give the Inn members "food for thought" about their own possible need to be more vigilant with their data. It will also serve to introduce topics such as metadata, scrubbing as well as ways to secure data. There will also be a speaker who specializes in cyber security in his practice in order to further develop these ideas and to give an indication as to best practices for attorneys as well as how to advise clients in the event of a breach that they need to defend in litigation.

Temple American Inn of Court April Team Script FINAL

Introduction:

I want you to all use your imagination and really dig deep to envision the scenario I'm about to describe for you. It may seem truly unimaginable. You may think it's far too out of touch with reality for you to believe it. So please, suspend all disbelief.

Picture it: 2017, a sun-soaked, warm-weather, estate, a National Historic Site formerly owned by legendary Washington hostess and heiress Marjorie Meriweather Post, somewhere in Florida. The site has since been turned in a private, see and be seen, dues charging, private members' golf club. It features, oh, about 120 rooms, runs about 110,000 square feet. Some people might consider it a wee ostentatious, but those old WASPy fuddy-duddies in Palm Beach have something to say about everything. Sad.

Our protagonist, Don, is a partner at a local law firm. Don's a real gregarious, fly by the seat of his pants, trust your gut, type of guy. He's spend the day golfing with one of his associates and some potential clients. The booze flowed freely in that hot Florida sun and sunscreen is for losers. Everyone's sunburned, hot, tired, and a little tipsy as they sit down for dinner. Don and his associate have avoided their phones all day – Don, because he can't be bothered with that thing anyway, and his associate because hey, a day doing this is better than a day at the office, and the other associates can handle that nonsense.

So you can imagine their shock to pull out their phones for the first time and see yet another case has blown up.

Skit 1 :

[*slide 1*]

Narrator: Don and Associate have spent the day golfing with potential clients. They're sunburned, tired, and a little tipsy. They sit down for dinner. These are mega-potential clients and therefore they've been avoiding being on their phones all day on other business. They're therefore shocked to pull them out and realize that another case has blown up.

[slide 2]

Associate 1: Oh my God.

Don: [*still gladhanding and shoving well-done steak into his mouth*]

Associate 1: Excuse me.

Don: Where are you going? We're going to close this deal! Stay at this table.

Associate 1: I need to use the restroom!

[*Associate walks away to check phone. Calls firm. Associate #2 picks up, in a panic*.]

Associate #2: The flux capacitator deal will fall apart if we don't get this cleared up by midnight. Where's Don?! What is Don doing?

Associate 1: Does it really need to be him? Where's Mike?!

Associate 2: He doesn't let Mike make these decisions! Where's Rosie?! Rosie is the one with his ear! He listens to Rosie! I don't want to make a decision without her input anyway, we'll all get fired.

Associate 1: Rosie is where she always is, lurking behind him as a dark shadow.

Associate 2: They both need to see these documents NOW. If this falls through you can kiss Multinational Corp. Tower's business good bye, anyway. We'll be toxic. Losers. Sad! It's all of the plans for the product itself, and Brown wants Don to review the financials and personal information of all of the potential investors. He says that's why he's hired him – his connections, not his ability.

Associate 1: OMG what if he tweets about us.

Associate 2: LOSERS. I will send you the M&A documents, the new demand, and the confidentiality agreement to your secured work phone. Do not forget, the flux capcitator requires plutonium and the NSA and CIA have been watching Brown Industries for months for a slipup. Make sure no one can see or hear you. And remember, the client information is all in there, too. He's got to review the potential investors and approve them. That includes everything – their social security numbers, their birthdates, their bank account information, even information on their debt loads. A treasure trove of personal information. Is the Wi-Fi there secure?

Associate 1: Yeah, all wi-fi is secure. It's been working perfectly all day. I just connected right to it when we got here. It was easy! Sheesh, stop with the questions.

Associate 2: ASK SOMEONE. You didn't put in a password? You've been using email all day on this? Did you review these documents on it?

Associate 1 to Associate 2: He won't use secure systems. You know that. What's the worst that can happen? It's not like the unsecured wi-fi is compromised and being monitored by multiple governments and mercenaries, all aware that Don does business with Doc Brown.

[*Associate 1 returns to the table. Associate 1 grabs a shadowy figure dressed in all black*.]

Associate 1: Rosie, there's a problem.

Rosie: This is the plan, it's all supposed to collapse. The world order is going to….

Associate 1: [*interrupts* Rosie] Yeah, I know, I get it, you're a Leninst, blah blah blah. This is more important; the flux deal is going to collapse unless we get Don's approval and sign-off on some snags. I need you to get him away from the table. The client that he's wooing can't see the documents. It's highly sensitive information, not only about our current client's products, but also about the investors and potential investors.

[*Rosie whispers in Don's ear*.]

Don: Well, bring them to me.

Associate 1: If you sign into secure systems on your work phone, you can read them securely.

Rosie: He doesn't know what secure systems is.

Don: I can't read the print on that thing anyway. My puny sausage fingers can't move the words. Just print them. Print them NOW. Rosie already had them sent for printing. Why are you useless and Rosie so wonderful, anticipating all of my needs? Sad!

[*Waiter appears with papers*]

Don: Everyone grab a seat! Let's make deals! Client, don't look.

Associate 1: This is confidential! The flux capacitor is not even on the market yet! And there's banking information all over these documents, plus proprietary information and personal information. You can't do that! We'll lose the client. And expose all of the personal information of his investors, too.

Don: Can't see! Too dark in here. I've never lost a deal, kid. We conducted this business like this all the time in my day. I've been making deals longer than you've been alive.

Client: My phone has a light, [*to the audience*] that is not at all conveniently located next to the camera! [*to Don*] Let me help. [*shines light]*

Don: Perfect! Waiter- do you have phone? Bring a light over here!

Client: [*to the audience*] Oh my God these are Doc Brown's flux capacitor prints! He finally got government approval?! [*starts snapping pictures*]

Don: Yep, this is the kind of major deal we can broker for you, too!

Client: [*to the audience]* These also have all of his investors' financial information! Wow, what a bonanza of potential for me!

Associate 1: What is that sound? Are you taking pictures?! You can't take pictures!

Client: Uhh thats just the noise the light makes.... Juuuustttt the light.

Rosie: There's cameras all over this club, whoever wants to see it can. Relax, kid, it'll be fine. Who's ever gotten in trouble for releasing private information or using a private email server? No one will look!

Don: Forgot to tweet my score from today.

[slide 3: *Mock-up Tweet is displayed on screen: Shot a 68! #makemygolfgamegreatagain (random numbers follow: 0600089989) Picture with the tweet will be the scorecard and then the documents with the personal info behind it, visible*.]

Don: Whoops, that's Jack's bank account number! I must have hit paste, instead. Somebody fix that.

----- END -----

Introduction: Now, this scene is a little different. Now we're in the office of a hiring partner at another local law firm. A young, go-getting attorney has applied for a job as an associate. Buuuut, our aspiring applicant emailed Microsoft Word versions, of his cover letter and resume to the hiring partner, and the firm's IT director, Marcy, was able to open the metadata therein. It showed all the other firms the applicant applied to and all of the edits to the documents. This offended our Partner, who believes that above all, he is the sun around which the planets orbit, and he's now prepared to confront the applicant about all of the information he gleaned from that data. However, our applicant might not be as naïve as he seems.

Skit 2

[*slide 4*]

Narrator: Sets the scene…

Mr. Darrow to secretary: Jean I'm ready for the scrub kid's interview. I cannot believe she had the gall to apply to 10 other law firms with 10 different resumes before she applied here. And the same cover letter every time! "It would be the dream of my life to work for your firm", blah blah blah. Kudos to Marcy from IT who showed me what metadata is. Man it is impossible to find decent candidates these days- I'd be better off hosting a game show to find a qualified applicant!

Secretary: "He's ready for you."

Applicant: Mr. Darrow, I just want to thank you for bringing me in for this honor. It would be an honor and privilege to work for such well-known fighters for justice as Darrow and Scopes.

Mr. Darrow: Look Kid, you applied to the securities group at John Marshall's law firm, the patent infringement group at Higginbotham's firm, the M&A group at Thurgood Marshall's firm – I could go on and on. And each time with a tailored resume but the same thing in your cover letter – what an honor and privilege and blah blah, brown-nosing crap- Did you even go to law school??

Applicant: Well, I, uh, I mean this time I mean it! I didn't mean it all those other times. How do you even know this?! Man, you really are the best. I never should have even applied to those other guys.

Mr Darrow: THE METADATA.

Applicant: the what?!

Mr. Darrow: The metadata! It tells you everything about a document. How many edits, what kind of edits, who you sent this to, it all hides in there in the document - or so says Marcy the IT lady.

Applicant: This sounds like surveillance! You broke into my document! You hacked my computer!

Mr. Darrow: NOPE. That is not what metadata is. It's all right there, in the document you sent me. Under metadata! Learn to scrub, kid. Jean!....Jean get me Marcy from IT up here! Where is she?! Stay put kid.

[*Darrow goes to look for secretary*]

[*When he gets up, he moves some documents on his desk, showing a file that says "DOC BROWN FLUX DEAL".*]

Applicant: I am so sick of getting lectured by these baby boomers about security. Now, where's that file. [*produces USB*]. Now that he opened my [*air quotes*] resume and overrode the Windows warnings about the file, my script already pulled all of the flux capacitator competitor information, and all I have to do is download it onto here. 10th law firm this week. And this guy's even more compromised than I thought. I wonder which Nigerian prince he gives money to… He must have no idea he responded to that phishing email. You know what? He's so stupid, I'm not even going to feel bad about this. I'm doing his clients a favor, frankly. They should know what a putz he is.

[*sounds of footsteps- Applicant quickly sits, but not before getting the whole file.*]

Mr. Darrow : Marcy's at lunch. Alright kid. Get out of my office. I can't handle your snowflake generation. And next time, do whatever that scrub thing is. Scrub the metadata.

Applicant: Thank you for this eye-opening experience!

----- END ----

<u>Skit 3</u>

[*slide 5*: *outside big tall glass law firm looking building (photo on screen):*]

Narrator: Sets the scene…

[*stage left*]

Associate 2: Did you see that tweet?

Associate 1: I don't want to think about it.

Associate 2: Do you think you could see anything? I think you could see that bit about the Libyans...

Associate 1: You can't see anything. My psychiatrist won't prescribe any more increases to my medication- so as far as I'm concerned you can't see a damn thing.

Associate 2: Shouldn't we at least give them a heads up?

Associate 1: Look we weren't the only ones with access to that information. Here have a happy pill. Better yet, take two.

[*stage right*]

Mr. Darrow: This is all your fault. You finalized the paperwork at your golf club!

Don: My fault!? Your puny firm doesn't have half of the fancy shmancy IT department security stuff we have!

Mr. Darrow: That fancy stuff only works if you ACTUALLY use it!

Don: Please! This is all a conspiracy created by the liberal media! If we keep repeating that enough times, it will be true. Trust me!

[*center stage*]

David Farenthold 2: We're here today for the press conference that's been called by major Multinational Law Firm. This is no doubt related to the law suit recently filed by Brown Industries against not only Multinational but also a smaller, local law firm. Brown accuses both firms of having deliberately leaked, or failed to protect, proprietary M&A information relating to Brown's top-secret invention of a flux capacitor.

Lawyer for Brown: The leak and reveal of my client's secret invention allowed competitors access to his life's work.

David Farenthold 2: Plus it led to Doc Brown's arrest for doing business with the Libyans for that plutonium needed to power it

Lawyer for Brown: ALLEGEDLY.

David Farenthold 2: We'll go live now to the press conference.

Reporter: [*To don*] Is it true you breached the security of your client by reviewing his privileged documents at a restaurant with another client"

Don: Uh no comment

Reporter 1: My source tells me that you did that and used an unsecure Wi-Fi network, care to comment?

Mr Darrow: We are investigating and will comment soon

Reporter 3: [To Don] Buzz feed has to know- is it true your hands are too small to use your secured phone!?

Don: My hands are great!

Reporter 2: It's my understanding that Doc Brown has reported you to the disciplinary board for violating Rule 1.6 because you failed to secure his documents and research and now his competitors are swooping in – can you comment on that?

Don: [Looks sheepishly at his feet]

Mr. Darrow: We will have more to say later.

Reporter 2: While were talking, Mr. Darrow, Isn't it true that you left your computer unattended and had sensitive data stolen from your firm as well?

Mr. Darrow: What?! Where are you getting your information… no comment

[Both Mr. Darrow and Don hurry off stage as they leave Mr. Darrow can be heard]

Mr. Darrow: Marcy... where are you.

Bibliography – What goes in cyberspace stays in cyber space… (Making cyber security a surety)

"Alleged Law Firm Hackers Hit with SEC Injunction" by William Gorta, Law360, (January 9, 2017).

"Chicago Firm Didn't secure client data, suit says" by Cara Salvatore, Law360 (December 9, 2016).

"NY Couple says attorney negligent for using AOL email" by Kat Green Law 360 (April 18 2016).

"Best Practices for Victim Response and Reporting of Cyber Incidents by Cyber security Unit, Computer Crime and Intellectual Property Section criminal division U.S. Department of Justice Version 1.0 (April 2015)

"Start with Security a guide for business – Lessons learned from FTC Cases; Federal Trade Commission, June 2015

Formal Opinion 2011-200 PA Bar Association Committee on Legal Ethics and Professional Responsibility

Applicable Rules of professional conduct Pennsylvania

WHAT GOES IN CYBERSPACE….

…..STAYS IN CYBER SPACE

(MAKING CYBER SECURITY A SURETY)

APRIL TEAM – TEMPLE INN OF COURT

Team Leaders:	Judge Marilyn Heffley Jacqueline Juliano Coelho, Esq
Script Writers:	Erin Lamb, Esq Samatha Mertz, Esq
Moderator:	Mark Lee, Esq
Guest Speaker:	Edward McAndrew, Esq

Skit 1—

Associate 1:	Alex Nasser, Esq
Partner:	Neil Morris, Esq
Associate 2:	Amanda Reed, Esq
Don:	Peter Thompson, Esq
Rosie:	Judge Ashely Chen
Client:	Nancy Mancheski, Esq
Reporter:	Anthony Provost, Esq
Waitress:	Victoria Ruby (student)

Skit 2—

Mr. Darrow:	Judge Christopher Mallios
Applicant:	Samatha Mertz, Esq
Gene:	Brian Chacker, Esq

Skit 3 –

Attorney for Brown:	David Dzara, Esq
Reporters:	James Kahn Esq, Jessica Stachelrodt (student)

GUEST SPEAKER

Edward J. McAndrew is a counselor, investigator, and trial lawyer who helps clients navigate life in the digital world. He is co-leader of Ballard Spahr's Privacy and Data Security Group.

Named a "Cybersecurity and Data Privacy Trailblazer" by *The National Law Journal*, Mr. McAndrew advises clients on cybersecurity, digital privacy, cyber-incident response, social media, online speech, defamation, commercial, employment, intellectual property, corporate governance, and regulatory compliance, and enforcement matters. He also advises clients on cyber-based national security issues, as well as governmental demands for third party data and assistance in investigations. Outside of the cyber arena, he handles civil and criminal investigations, litigation, and trials in various substantive areas.

April 12, 2017

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Alleged Law Firm Hackers Hit With SEC Injunction

By **William Gorta**

Law360, New York (January 9, 2017, 6:45 PM EST) -- A New York federal judge on Monday granted a request by the U.S. Securities and Exchange Commission for a preliminary injunction and asset freeze against four Chinese hackers accused of reaping $4 million in illegal profits using insider information about pending corporate deals hacked from the computer systems of two top New York law firms.

U.S. District Judge Valerie Caproni's order said that given the SEC's likelihood of prevailing at trial, the four were enjoined violating the Exchange Act and ordered not to conceal, transfer or spend assets that may be subject to disgorgement. They were also ordered to repatriate any money taken out of the country and to preserve documents and records.

Judge Caproni had already granted a similar temporary restraining order against alleged hackers Iat Hong, Bo Zheng and Hung Chin, along with Sou Cheng Lai, Hong's mother, a relief defendant in the civil suit. Hong, Zheng and Chin also face related criminal charges. Hong was arrested in Hong Kong on Christmas Day.

None of the civil defendants was in court Monday.

In an announcement unsealing the criminal charges Dec. 27, U.S. Attorney Preet Bharara of the Southern District of New York said the men purchased shares in at least five publicly traded companies based on confidential information that they obtained in emails stolen from two law firms' servers between April 2014 and late 2015.

The scheme, which targeted at least seven U.S.-based international law firms with New York offices that advise companies on mergers and acquisitions, saw the defendants buy stocks that were expected to increase in value once certain mergers were announced and then sell those shares for several million dollars in profit after the acquisitions were made public, the indictment said.

The men are accused of stealing as much as 10 gigabytes of confidential data from a single server.

The names of the law firms were not disclosed.

The men also worked at a robotics start-up started by Zheng and also hacked other robotics companies, allegedly stealing confidential schematic designs, the indictment said.

Hong, 26, his mother Lai, 47, and Hung, 50, are residents of Macau. Zheng, 30, is a resident of Changsha, China.

Counsel for the defendants was not immediately available.

The SEC is represented by Jennie Boehm Krasner, Britt Biles and Brittany Whitesell Biles.

The case is U.S. Securities and Exchange Commission v. Hong et al., case number 1:16-cv-09947, in the U.S. District Court for the Southern District of New York.

--Additional reporting by Kat Sieniuc. Editing by Sara Ziegler.

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Chicago Firm Didn't Secure Client Data, Suit Says

By **Cara Salvatore**

Law360, New York (December 9, 2016, 6:38 PM EST) -- Former clients of Illinois law firm Johnson & Bell Ltd. are accusing the firm of exposing client information and failing to protect client data, saying the firm has structural holes in its security architecture, in a proposed class action unsealed Friday.

Coinabul LLC and Jason Shore were clients of the 100-attorney firm from August 2014 to February 2015, according to the suit, which was filed in April under seal.

"Defendant's computer systems suffer from critical vulnerabilities in its internet-accessible web services," the suit says. "As a result, confidential information entrusted to Johnson & Bell by its clients has been exposed and is at great risk of further unauthorized disclosure (if it hasn't already been disclosed)."

This revelation came from public information, the suit says.

One vulnerability detailed in the suit is the firm's internet-based time-logging system, JBoss, which is 10 years old and a popular target of hackers because of its known vulnerabilities, the suit claims. It also says the firm's virtual private network, or VPN, is insecure, and so is its private email server, which the ex-clients say can be exploited by the same hack that exposed the Panama Papers.

Meanwhile, the firm holds itself out as having expertise in cybersecurity, the suit says, citing an article by two partners.

One of them, Joseph Marconi, said Friday that the suit doesn't allege that any actual breach has occurred. And founder and president William Johnson said they will strike back against the plaintiffs.

"Our data systems are secure and our clients' information is protected," Johnson said in a statement. "We will fully defend our firm against this baseless lawsuit and will seek appropriate action against plaintiffs after the lawsuit is concluded."

The firm has asked the court to dismiss the case. "If plaintiffs' claims are actionable, then every lawyer who carries a briefcase, takes notes in court or in a deposition, or speaks with his or her client in public could be subject to being named in a class action lawsuit because in each instance a client's confidential information was 'exposed' or 'vulnerable,'" its motion said.

The plaintiffs are represented by Jay Edelson, Amir Missaghi, Benjamin Richman, Benjamin Thomassen, Rafey Balabanian, and Todd Logan of Edelson PC.

Johnson & Bell is represented by Michael Bruck of Williams Montgomery & John Ltd.

The case is Shore et al. v. Johnson & Bell Ltd., case number 1:16-cv-04363, in the U.S. District Court for the Northern District of Illinois.

--Editing by Brian Baresch.

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NY Couple Says Attorney Negligent For Using AOL Email

By **Kat Greene**

Law360, Los Angeles (April 18, 2016, 9:39 PM EDT) -- A New York couple accused their real estate attorney of negligently using a "notoriously vulnerable" AOL email account that was hacked by cybercriminals who then stole nearly $2 million from the couple, according to a state court suit filed Monday.

Robert and Bethany Millard accused attorney Patricia L. Doran of breaching her duties to her clients by using an AOL email account and failing to install even basic protective add-ons to improve the security of her email, according to their suit filed in New York state court. Her computer itself also "was poorly configured" and had malware on it enabling thieves to access her passwords and files, the Millards said.

The problem came to light when the Millards received an email they thought was from Doran directing the couple to wire about $1.9 million to an account as a deposit for the new apartment they were trying to buy in Manhattan, according to the suit. Doran even forwarded the couple a confirmation she received on the deposit, but she didn't check whether the money had gone to the right place, the couple said.

"AOL email accounts are notoriously vulnerable to 'hacking' by 'cybercriminals,'" the couple said in the suit. "Doran's negligence in failing to protect the integrity of both her email system and her computer system, and her failure to take the most basic steps to confirm that the funds wired by her clients actually were received by the seller's attorneys, enabled the cybercriminals to successfully accomplish their scheme."

In the fall of 2015, the Millards made an oral offer on a cooperative apartment in Manhattan, and in November, the parties adopted a deal sheet that set the price at $19.4 million, according to the complaint.

The couple hired Doran to represent them in the deal, but she never prepared an engagement letter or any other document outlining her duties, they said.

For her law practice, Doran uses an AOL email account, the couple said. Those accounts have "a number of substandard features," including a lack of several backstops that would prevent hackers from gaining access, they said.

Doran also didn't install basic cybersecurity protection on the computer she used to conduct business, the couple said in the suit. The action had predictable results: cybercriminals accessed the Millards' information, figured out the couple were about to make a hefty deposit, then stepped in to pose as the seller's attorneys to steal the money, according to the suit.

The Millards were able to recover most of their money "without Doran's help" but are still short about $196,200, they said. They're seeking that amount, plus punitive damages, fees and costs, in Monday's complaint.

Doran didn't immediately respond to a request for comment late Monday.

The Millards are represented by John T. Bandler of Bandler Law Firm PLLC.

Counsel information for Doran couldn't be immediately determined.

The case is Robert Millard et al. v. Patricia L. Doran, case number 153262/2016, in the Supreme Court of the State of New York, County of New York.

--Editing by Catherine Sum.

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents

Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* an incident occurs.

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may benefit from it.

I. Steps to Take *Before* a Cyber Intrusion or Attack Occurs

Having well-established plans and procedures in place for managing and responding to a cyber intrusion or attack is a critical first step toward preparing an organization to weather a cyber incident. Such pre-planning can help victim organizations limit damage to their computer networks, minimize work stoppages, and maximize the ability of law enforcement to locate and apprehend perpetrators. Organizations should take the precautions outlined below before learning of a cyber incident affecting their networks.

A. Identify Your "Crown Jewels"

Different organizations have different mission critical needs. For some organizations, even a short-term disruption in their ability to send or receive email will have a devastating impact on their operations; others are able to rely on other means of communication to transact

business, but they may suffer significant harm if certain intellectual property is stolen. For others still, the ability to guarantee the integrity and security of the data they store and process, such as customer information, is vital to their continued operation.

The expense and resources required to protect a whole enterprise may force an organization to prioritize its efforts and may shape its incident response planning. Before formulating a cyber incident response plan, an organization should first determine which of their data, assets, and services warrants the most protection. Ensuring that protection of an organization's "crown jewels" is appropriately prioritized is an important first step to preventing a cyber intrusion or attack from causing catastrophic harm. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) provides excellent guidance on risk management planning and policies and merits consideration.[1]

B. Have an Actionable Plan in Place Before an Intrusion Occurs

Organizations should have a plan in place for handling computer intrusions before an intrusion occurs. During an intrusion, an organization's management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the damage and the potential source of the threat. A cyber incident is not the time to be creating emergency procedures or considering for the first time how best to respond.

The plan should be "actionable." It should provide specific, concrete procedures to follow in the event of a cyber incident. At a minimum, the procedures should address:

- Who has lead responsibility for different elements of an organization's cyber incident response, from decisions about public communications, to information technology access, to implementation of security measures, to resolving legal questions;
- How to contact critical personnel at any time, day or night;
- How to proceed if critical personnel is unreachable and who will serve as back-up;
- What mission critical data, networks, or services should be prioritized for the greatest protection;
- How to preserve data related to the intrusion in a forensically sound manner;
- What criteria will be used to ascertain whether data owners, customers, or partner companies should be notified if their data or data affecting their networks is stolen; and
- Procedures for notifying law enforcement and/or computer incident-reporting organization.

[1] The NIST Cybersecurity Framework is available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

All personnel who have computer security responsibilities should have access to and familiarity with the plan, particularly anyone who will play a role in making technical, operational, or managerial decisions during an incident. It is important for an organization to institute rules that will ensure its personnel have and maintain familiarity with its incident response plan. For instance, the procedures for responding to a cyber incident under an incident response plan can be integrated into regular personnel training. The plan may also be ingrained through regularly conducted exercises to ensure that it is up-to-date. Such exercises should be designed to verify that necessary lines of communication exist, that decision-making roles and responsibilities are well understood, and that any technology that may be needed during an actual incident is available and likely to be effective. Deficiencies and gaps identified during an exercise should be noted for speedy resolution.

Incident response plans may differ depending upon an organization's size, structure, and nature of its business. Similarly, decision-making under a particular incident response plan may differ depending upon the nature of a cyber incident. In any event, institutionalized familiarity with the organization's framework for addressing a cyber incident will expedite response time and save critical minutes during an incident.

C. Have Appropriate Technology and Services in Place Before An Intrusion Occurs

Organizations should already have in place or have ready access to the technology and services that they will need to respond to a cyber incident. Such equipment may include off-site data back-up, intrusion detection capabilities, data loss prevention technologies, and devices for traffic filtering or scrubbing. An organization's computer servers should also be configured to conduct the logging necessary to identify a network security incident and to perform routine back-ups of important information. The requisite technology should already be installed, tested, and ready to deploy. Any required supporting services should either be acquired beforehand or be identified and ready for acquisition.

D. Have Appropriate Authorization in Place to Permit Network Monitoring

Real-time monitoring of an organization's *own* network is typically lawful if prior consent for such monitoring is obtained from network users. For this reason, before an incident takes place, an organization should adopt the mechanisms necessary for obtaining user consent to monitoring users' communications so it can detect and respond to a cyber incident. One means of accomplishing this is through network warnings or "banners" that greet users who log onto a network and inform them of how the organization will collect, store, and use their communications. A banner can also be installed on the ports through which an intruder is likely to access the organization's system.

A banner, however, is not the only means of obtaining legally valid consent. Computer user agreements, workplace policies, and personnel training may also be used to obtain legally sufficient user consent to monitoring. Organizations should obtain written acknowledgement from their personnel of having signed such agreements or received such training. Doing so will provide an organization with ready proof that they have met legal requirements for conducting network monitoring.

Any means of obtaining legally sufficient consent should notify users that their use of the system constitutes consent to the interception of their communications and that the results of such monitoring may be disclosed to others, including law enforcement.[2] If an organization is a government entity (*e.g.*, a federal, state, or local agency or a state university) or a private entity acting as an instrument or agent of the government, its actions may implicate the Fourth Amendment. Consequently, any notice on the system of such an entity or organization should also inform users of their diminished expectation of privacy for communications on the network.

E. Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident

Cyber incidents can raise unique legal questions. An organization faced with decisions about how it interacts with government agents, the types of preventative technologies it can lawfully use, its obligation to report the loss of customer information, and its potential liability for taking specific remedial measures (or failing to do so) will benefit from obtaining legal guidance from attorneys who are conversant with technology and knowledgeable about relevant laws (*e.g.*, the Computer Fraud and Abuse Act (18 U.S.C. § 1030), electronic surveillance, and communications privacy laws). Legal counsel that is accustomed to addressing these types of issues that are often associated with cyber incidents will be better prepared to provide a victim organization with timely, accurate advice.

Many private organizations retain outside counsel who specialize in legal questions associated with data breaches while others find such cyber issues are common enough that they have their own cyber-savvy attorneys on staff in their General Counsel's offices. Having ready access to advice from lawyers well acquainted with cyber incident response can speed an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing.

---

[2] More guidance on banners, including a model banners, can be found in our manual on searching and seizing electronic evidence and in a 2009 legal opinion prepared by the Department of Justice's Office of Legal Counsel. *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed. 2009), available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; and Stephen G. Bradbury, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, 33 Op. Off. Legal Counsel 1 (2009), available at http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf.

F. Ensure Organization Policies Align with Your Cyber Incident Response Plan

Some preventative and preparatory measures related to incident planning may need to be implemented outside the context of preparing a cyber incident response plan. For instance, an organization should review its personnel and human resource policies to ensure they will reasonably minimize the risk of cyber incidents, including from "insider threats." Proper personnel and information technology (IT) policies may help prevent a cyber incident in the first place. For instance, a practice of promptly revoking the network credentials of terminated employees—particularly system administrators and information technology staff—may prevent a subsequent cyber incident from occurring. Furthermore, reasonable access controls on networks may reduce the risk of harmful computer misuse.

G. Engage with Law Enforcement Before an Incident

Organizations should attempt to establish a relationship with their local federal law enforcement offices long before they suffer a cyber incident. Having a point-of-contact and a pre-existing relationship with law enforcement will facilitate any subsequent interaction that may occur if an organization needs to enlist law enforcement's assistance. It will also help establish the trusted relationship that cultivates bi-directional information sharing that is beneficial both to potential victim organizations and to law enforcement. The principal federal law enforcement agencies responsible for investigating criminal violations of the federal Computer Fraud and Abuse Act are the Federal Bureau of Investigation (FBI) and the U.S. Secret Service. Both agencies conduct regular outreach to private companies and other organizations likely to be targeted for intrusions and attacks. Such outreach occurs mostly through the FBI's Infragard chapters and Cyber Task Forces in each of the FBI's 56 field offices, and through the U.S. Secret Service's Electronic Crimes Task Forces.

H. Establish Relationships with Cyber Information Sharing Organizations

Defending a network at all times from every cyber threat is a daunting task. Access to information about new or commonly exploited vulnerabilities can assist an organization prioritize its security measures. Information sharing organizations for every sector of the critical infrastructure exist to provide such information. Information Sharing and Analysis Centers (ISACs) have been created in each sector of the critical infrastructure and for key resources. They produce analysis of cyber threat information that is shared within the relevant sector, with other sectors, and with the government. Depending upon the sector, they may also provide other cybersecurity services. The government has also encouraged the creation of new information sharing entities called Information Sharing and Analysis Organizations (ISAOs) to accommodate organizations that do not fit within an established sector of the critical infrastructure or that have

unique needs.[3] ISAOs are intended to provide such organizations with the same benefits of obtaining cyber threat information and other supporting services that are provided by an ISAC.

II. Responding to a Computer Intrusion: Executing Your Incident Response Plan

An organization can fall victim to a cyber intrusion or attack even after taking reasonable precautions. Consequently, having a vetted, actionable cyber incident response plan is critical. A robust incident response plan does more than provide procedures for handling an incident; it also provides guidance on how a victim organization can continue to operate while managing an incident and how to work with law enforcement and/or incident response firms as an investigation is conducted.[4] An organization's incident response plan should, at a minimum, give serious consideration to all of the steps outlined below.

A. Step 1: Make an Initial Assessment

During a cyber incident, a victim organization should immediately make an assessment of the nature and scope of the incident. In particular, it is important at the outset to determine whether the incident is a malicious act or a technological glitch. The nature of the incident will determine the type of assistance an organization will need to address the incident and the type of damage and remedial efforts that may be required.

Having appropriate network logging capabilities enabled can be critical to identifying the cause of a cyber incident. Using log information, a system administrator should attempt to identify:

- The affected computer systems;
- The apparent origin of the incident, intrusion, or attack;
- Any malware used in connection with the incident;
- Any remote servers to which data were sent (if information was exfiltrated); and
- The identity of any other victim organizations, if such data is apparent in logged data.

[3] *See*, Exec. Order No. 13,691, 80 Fed. Reg. 9347 (Feb. 20, 2015), available at http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[4] Often in the case of data breaches, organizations may learn that they have been the victim of an intrusion from a third party. For instance, law enforcement may discover evidence; while conducting a data breach investigation that other organizations have also been breached, or a cybersecurity company's forensic analysis of a customer's network following a breach may uncover evidence of other victims. Organizations should be prepared to respond to such receiving such notice.

In addition, the initial assessment of the incident should document:

- Which users are currently logged on;
- What the current connections to the computer systems are;
- Which processes are running; and
- All open ports and their associated services and applications.

Any communications (in particular, threats or extortionate demands) received by the organization that might relate to the incident should also be preserved. Suspicious calls, emails, or other requests for information should be treated as part of the incident.

Evidence that an intrusion or other criminal incident has occurred will typically include logging or file creation data indicating that someone improperly accessed, created, modified, deleted, or copied files or logs; changed system settings; or added or altered user accounts or permissions. In addition, an intruder may have stored "hacker tools" or data from another intrusion on your network. In the case of a root-level intrusion,[5] victims should be alert for signs that the intruder gained access to multiple areas of the network. The victim organization should take care to ensure that its actions do not unintentionally or unnecessarily modify stored data in a way that could hinder incident response or subsequent criminal investigation. In particular, potentially relevant files should not be deleted; if at all possible, avoid modifying data or at least keep track of how and when information was modified.

B. Step 2: Implement Measures to Minimize Continuing Damage

After an organization has assessed the nature and scope of the incident and determined it to be an intentional cyber intrusion or attack rather than a technical glitch, it may need to take steps to stop ongoing damage caused by the perpetrator. Such steps may include rerouting network traffic, filtering or blocking a distributed denial-of-service attack,[6] or isolating all or parts of the compromised network. In the case of an intrusion, a system administrator may decide either to block further illegal access or to watch the illegal activity to identify the source of the attack and/or learn the scope of the compromise.

If proper preparations were made, an organization will have an existing back-up copy of critical data and may elect to abandon the network in its current state and to restore it to a prior

[5] An intruder with "root level access" has the highest privileges given to a user working with an operating system or other program and has as much authority on the network as a system administrator, including the authority to access files, alter permissions and privileges, and add or remove accounts.

state. If an organization elects to restore a back-up version of its data, it should first make sure that the back-up is not compromised as well.

Where a victim organization obtains information regarding the location of exfiltrated data or the apparent origin of a cyber attack, it may choose to contact the system administrator of that network. Doing so may stop the attack, assist in regaining possession of stolen data, or help determine the true origin of the malicious activity. A victim organization may also choose to blunt the damage of an ongoing intrusion or attack by "null routing"[7] malicious traffic, closing the ports being used by the intruder to gain access to the network, or otherwise altering the configuration of a network to thwart the malicious activity.

The victim organization should keep detailed records of whatever steps are taken to mitigate the damage and should keep stock of any associated costs incurred. Such information may be important for recovering damages from responsible parties and for any subsequent criminal investigation.

C. Step 3: Record and Collect Information

1. *Image the Affected Computer(s)*

Ideally, a victim organization will immediately make a "forensic image" of the affected computers, which will preserve a record of the system at the time of the incident for later analysis and potentially for use as evidence at trial.[8] This may require the assistance of law enforcement or professional incident response experts. In addition, the victim organization should locate any previously generated backups, which may assist in identifying any changes an intruder made to the network. New or sanitized media should be used to store copies of any data that is retrieved and stored. Once the victim organization makes such copies, it should write-protect the media to safeguard it from alteration. The victim organization should also restrict access to this media to maintain the integrity of the copy's authenticity, safeguard it from unidentified malicious insiders, and establish a chain of custody. These steps will enhance the value of any backups as evidence in any later criminal investigations and prosecutions, internal

---

[6] A Distributed Denial of Service (DDOS) attack involves the orchestrated transmission of communications engineered to overwhelm another network's connection to the Internet to impair or disrupt that network's ability to send or receive communications. DDOS attacks are usually launched by a large number of computers infected by malware that permits their actions to be centrally controlled.

[7] A null route directs the system to drop network communications that are destined for specified IP address on the network, so a system will no longer send any response to the originating IP address. This means the system will continue to receive data from the attackers but no longer respond to them.

[8] A "forensic image" is an exact, sector-by-sector copy of a hard disk. Software capable of creating such copies of hard drives preserve deleted files, slack space, system files, and executable files and can be critical for later analysis of an incident.

investigations, or civil law suits.

2. *Keep Logs, Notes, Records, and Data*

The victim organization should take immediate steps to preserve relevant existing logs. In addition, the victim organization should direct personnel participating in the incident response to keep an ongoing, written record of all steps undertaken. If this is done while responding to the incident or shortly thereafter, personnel can minimize the need to rely on their memories or the memories of others to reconstruct the order of events. As the investigation progresses, information that was collected by the organization contemporaneous to the intrusion may take on unanticipated significance.

The types of information that the victim organization should retain include:

- a description of all incident-related events, including dates and times;
- information about incident-related phone calls, emails, and other contacts;
- the identity of persons working on tasks related to the intrusion, including a description, the amount of time spent, and the approximate hourly rate for those persons' work;
- identity of the systems, accounts, services, data, and networks affected by the incident and a description of how these network components were affected;
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the organization and in criminal cases;
- information regarding network topology;
- the type and version of software being run on the network; and
- any peculiarities in the organization's network architecture, such as proprietary hardware or software.

Ideally, a single, designated employee will retain custody of all such records. This will help to ensure that records are properly preserved and can be produced later on. Proper handling of this information is often useful in rebutting claims in subsequent legal proceedings (whether criminal or civil) that electronic evidence has been tampered with or altered.

3. Records Related to Continuing Attacks

When an incident is ongoing (*e.g.*, during a DDOS attack, as a worm is propagating through the network, or while an intruder is exfiltrating data), the victim organization should record any continuing activity. *If a victim organization has not enabled logging on an affected*

server, it should do so immediately. It should also consider increasing the default size of log files on its servers to prevent losing data. A victim organization may also be able to use a "sniffer" or other network-monitoring device to record communications between the intruder and any of its targeted servers. Such monitoring, which implicates the Wiretap Act (18 U.S.C. §§ 2510 et seq.) is typically lawful, provided it is done to protect the organization's rights or property or system users have actually or impliedly consented to such monitoring. An organization should consult with its legal counsel to make sure such monitoring is conducted lawfully and consistent with the organization's employment agreements and privacy policies.

D. Step 4: Notify[9]

1. *People Within the Organization*

Managers and other personnel within the organization should be notified about the incident as provided for in the incident response plan and should be given the results of any preliminary analysis. Relevant personnel may include senior management, IT and physical security coordinators, communications or public affairs personnel, and legal counsel. The incident response plan should set out individual points-of-contact within the organization and the circumstances in which they should be contacted.

2. Law Enforcement

If an organization suspects at any point during its assessment or response that the incident constitutes criminal activity, it should contact law enforcement immediately. Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harboring such concerns should not hesitate to contact law enforcement.

The FBI and U.S. Secret Service place a priority on conducting cyber investigations that cause as little disruption as possible to a victim organization's normal operations and recognize the need to work cooperatively and discreetly with victim companies. They will use investigative measures that avoid computer downtime or displacement of a company's employees. When using an indispensable investigative measures likely to inconvenience a victim organization, they will do so with the objective of minimizing the duration and scope of any disruption.

The FBI and U.S. Secret Service will also conduct their investigations with discretion and

[9] Some private organizations are regulated by the federal government and may be subject to rules requiring notification if a data breach or other cyber incident occurs. While guidance to such organizations for notifying regulators is beyond the scope of this document, a cyber incident response plan should take into account whether a victim organization may need also to notify regulators and how best to do so.

work with a victim company to avoid unwarranted disclosure of information. They will attempt to coordinate statements to the news media concerning the incident with a victim company to ensure that information harmful to a company's interests is not needlessly disclosed. Victim companies should likewise consider sharing press releases regarding a cyber incident with investigative agents before issuing them to avoid releasing information that might damage the ongoing investigation.

Contacting law enforcement may also prove beneficial to a victim organization. Law enforcement may be able to use legal authorities and tools that are unavailable to non-governmental entities[10] and to enlist the assistance of international law enforcement partners to locate stolen data or identify the perpetrator. These tools and relationships can greatly increase the odds of successfully apprehending an intruder or attacker and securing lost data. In addition, a cyber criminal who is successfully prosecuted will be prevented from causing further damage to the victim company or to others, and other would-be cyber criminals may be deterred by such a conviction.

In addition, as of January 2015, at least forty-seven states have passed database breach notification laws requiring companies to notify customers whose data is compromised by an intrusion; however, many data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice would impede an investigation. State laws also may allow a victim company to forgo providing notice altogether if the victim company consults with law enforcement and thereafter determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Organizations should consult with counsel to determine their obligations under state data breach notification laws. It is also noteworthy that companies from regulated industries that cooperate with law enforcement may be viewed more favorably by regulators looking into a data breach.

3. The Department of Homeland Security

The Department of Homeland Security has components dedicated to cybersecurity that not only collect and report on cyber incidents, phishing, malware, and other vulnerabilities, but also provide certain incident response services. The National Cybersecurity & Communications Integration Center (NCCIC) serves as a 24x7 centralized location for cybersecurity information sharing, incident response, and incident coordination. By contacting the NCCIC, a victim organization can both share and receive information about an ongoing incident that may prove beneficial to both the victim organization and the government. A victim organization may also

[10] For instance, data that are necessary to trace an intrusion or attack to its source may not be obtainable without use of legal process (e.g., a search warrant, court order, or subpoena) that may be unavailable to a private party. Furthermore, some potentially useful intrusion detection techniques require law enforcement involvement. For instance, under 18 U.S.C. § 2511(2)(i) a network owner may authorize law enforcement to intercept a computer trespasser's communications on the network owner's computers during an investigation.

obtain technical assistance capable of mitigating an ongoing cyber incident.

4. *Other Potential Victims*

If a victim organization or the private incident response firm it hires uncovers evidence of additional victims while assessing a cyber incident—for example, in the form of another company's data stored on the network—the other potential victims should be promptly notified. While the initial victim can conduct such notification directly, notifying victims through law enforcement may be preferable. It insulates the initial victim from potentially unnecessary exposure and allows law enforcement to conduct further investigation, which may uncover additional victims warranting notification. Similarly, if a forensic examination reveals an unreported software or hardware vulnerability, the victim organization should make immediate notification to law enforcement or the relevant vendor.

Such notifications may prevent further damage by prompting the victims or vendors to take remedial action immediately. The victim organization may also reap benefits, because other victims may be able to provide helpful information gleaned from their own experiences managing the same cyber incident (*e.g.*, information regarding the perpetrator's methods, a timeline of events, or effective mitigation techniques that may thwart the intruder).

III. What Not to Do Following a Cyber Incident

A. Do Not Use the Compromised System to Communicate

The victim organization should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about an incident or to discuss its response to the incident. If the victim organization must use the compromised system to communicate, it should encrypt its communications. To avoid becoming the victim of a "social engineering" attack (*i.e.*, attempts by a perpetrator to convince a target to take an action through use of a ruse or guile that will compromise the security of the system or data), employees of the victim organization should not disclose incident-specific information to unknown communicants inquiring about an incident without first verifying their identity.

B. Do Not Hack Into or Damage Another Network

A victimized organization should not attempt to access, damage, or impair another system that may appear to be involved in the intrusion or attack. Regardless of motive, doing so is likely illegal, under U.S. and some foreign laws, and could result in civil and/or criminal liability. Furthermore, many intrusions and attacks are launched from compromised systems. Consequently, "hacking back" can damage or impair another innocent victim's system rather

than the intruder's.

IV. After a Computer Incident

Even after a cyber incident appears to be under control, remain vigilant. Many intruders return to attempt to regain access to networks they previously compromised. It is possible that, despite best efforts, a company that has addressed known security vulnerabilities and taken all reasonable steps to eject an intruder has nevertheless not eliminated all of the means by which the intruder illicitly accessed the network. Continue to monitor your system for anomalous activity.

Once the victim organization has recovered from the attack or intrusion, it should initiate measures to prevent similar attacks. To do so, it should conduct a post-incident review of the organization's response to the incident and assess the strengths and weaknesses of its performance and incident response plan. Part of the assessment should include ascertaining whether the organization followed each of the steps outlined above and, if not, why not. The organization should note and discuss deficiencies and gaps in its response and take remedial steps as needed.

Cyber Incident Preparedness Checklist

Before a Cyber Attack or Intrusion

- Identify mission critical data and assets (*i.e.*, your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.
- Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.
- Create an actionable incident response plan.
    - Test plan with exercises
    - Keep plan up-to-date to reflect changes in personnel and structure
- Have the technology in place (or ensure that it is easily obtainable) that will be used to address an incident.
- Have procedures in place that will permit lawful network monitoring.
- Have legal counsel that is familiar with legal issues associated with cyber incidents
- Align other policies (*e.g.*, human resources and personnel policies) with your incident response plan.
- Develop proactive relationships with relevant law enforcement agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may require in the event of an incident.

During a Cyber Attack or Intrusion

- Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.
- Minimize continuing damage consistent with your cyber incident response plan.
- Collect and preserve data related to the incident.
    - "Image" the network
    - Keep all logs, notes, and other records
    - Keep records of ongoing attacks
- Consistent with your incident response plan, notify—
    - Appropriate management and personnel within the victim organization should
    - Law enforcement
    - Other possible victims
    - Department of Homeland Security
- Do not—
    - Use compromised systems to communicate.
    - "Hack back" or intrude upon another network.

After Recovering from a Cyber Attack or Intrusion

- Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.
- Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.

START WITH SECURITY

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

FEDERAL TRADE COMMISSION

START WITH SECURITY

1. **Start with security.**
2. **Control access to data sensibly.**
3. **Require secure passwords and authentication.**
4. **Store sensitive personal information securely and protect it during transmission.**
5. **Segment your network and monitor who's trying to get in and out.**
6. **Secure remote access to your network.**
7. **Apply sound security practices when developing new products.**
8. **Make sure your service providers implement reasonable security measures.**
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**
10. **Secure paper, physical media, and devices.**

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlined in *Protecting Personal Information: A Guide for Business,* you should know what personal information you have in your files and on your computers, and keep only what you need for your business. You should protect the information that you keep, and properly dispose of what you no longer need. And, of course, you should create a plan to respond to security incidents.

In addition to *Protecting Personal Information*, the FTC has resources to help you think through how those principles apply to your business. There's an online tutorial to help train your employees; publications to address particular data security challenges; and news releases, blog posts, and guidance to help you identify – and possibly prevent – pitfalls.

There's another source of information about keeping sensitive data secure: the lessons learned from the more than 50 law enforcement actions the FTC has announced so far. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1 Start with security.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. Experts agree on the key first step: Start with security. Factor it into the decisionmaking in every department of your business – personnel, sales, accounting, information technology, etc. Collecting and maintaining information "just because" is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business. Lessons from FTC cases illustrate the benefits of building security in from the start by going lean and mean in your data collection, retention, and use policies.

Don't collect personal information you don't need.

Here's a foundational principle to inform your initial decision-making: No one can steal what you don't have. When does your company ask people for sensitive information? Perhaps when they're registering online or setting up a new account. When was the last time you looked at that process to make sure you really need everything you ask for? That's the lesson to learn from a number of FTC cases. For example, the FTC's complaint against ***RockYou*** charged that the company collected lots of information during the site registration process, including the user's email address and email password. By collecting email passwords – not something the business needed – and then storing them in clear text, the FTC said the company created an unnecessary risk to people's email accounts. The business could have avoided that risk simply by not collecting sensitive information in the first place.

Hold on to information only as long as you have a legitimate business need.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the FTC's ***BJ's Wholesale Club*** case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

Don't use personal information when it's not necessary.

You wouldn't juggle with a Ming vase. Nor should businesses use personal information in contexts that create unnecessary risks. In the ***Accretive*** case, the FTC alleged that the company used real people's personal information in employee training sessions, and then failed to remove the information from employees' computers after the sessions were over. Similarly, in ***foru International***, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.

2 Control access to data sensibly.

Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. You'll want to keep it from the prying eyes of outsiders, of course, but what about your own employees? Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need to know" basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. When thinking about how to control access to sensitive information in your possession, consider these lessons from FTC cases.

Restrict access to sensitive data.

If employees don't have to use personal information as part of their job, there's no need for them to have access to it. For example, in ***Goal Financial***, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people's personal information.

Limit administrative access.

Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job. In its action against ***Twitter***, for example, the FTC alleged that the company granted almost all of its employees administrative control over Twitter's system, including the ability to reset user account passwords, view users' nonpublic tweets, and send tweets on users' behalf. According to the complaint, by providing administrative access to just about everybody in-house, Twitter increased the risk that a compromise of any of its employees' credentials could result in a serious breach. How could the company have reduced that risk? By ensuring that employees' access to the system's administrative controls was tailored to their job needs.

3 Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password "hygiene" – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are tips to take from FTC cases.

Insist on complex and unique passwords.

"Passwords" like 121212 or qwerty aren't much better than no passwords at all. That's why it's wise to give some thought to the password standards you implement. In the ***Twitter*** case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

Store passwords securely.

Don't make it easy for interlopers to access passwords. In ***Guidance Software***, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in ***Reed Elsevier***, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In ***Twitter***, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. In each of those cases, the risks could have been reduced if the companies had policies and procedures in place to store credentials securely. Businesses also may want to consider other protections – two-factor authentication, for example – that can help protect against password compromises.

Guard against brute force attacks.

Remember that adage about an infinite number of monkeys at an infinite number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password. In the ***Lookout Services***, ***Twitter***, and ***Reed Elsevier*** cases, the FTC alleged that the businesses didn't suspend or disable user credentials after a certain number of unsuccessful login attempts. By not adequately restricting the number of tries, the companies placed their networks at risk. Implementing a policy to suspend or disable accounts after repeated login attempts would have helped to eliminate that risk.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is left open. In ***Lookout Services***, the FTC charged that the company failed to adequately test its web application for widely-known security flaws, including one called "predictable resource location." As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

4 Store sensitive personal information securely and protect it during transmission.

For many companies, storing sensitive data is a business necessity. And even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. But regardless of the method, it's only as good as the personnel who implement it. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. With that in mind, here are a few lessons from FTC cases to consider when securing sensitive information during storage and transmission.

Keep sensitive information secure throughout its lifecycle.

Data doesn't stay in one place. That's why it's important to consider security at all stages, if transmitting information is a necessity for your business. In ***Superior Mortgage Corporation***, for example, the FTC alleged that the company used SSL encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, and not just during the initial transmission.

Use industry-tested and accepted methods.

When considering what technical standards to follow, keep in mind that experts already may have developed effective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary. Instead, they take advantage of that collected wisdom. The ***ValueClick*** case illustrates that principle. According to the FTC, the company stored sensitive customer information collected through its e-commerce sites in a database that used a non-standard, proprietary form of encryption. Unlike widely-accepted encryption algorithms that are extensively tested, the complaint charged that ValueClick's method used a simple alphabetic substitution system subject to significant vulnerabilities. The company could have avoided those weaknesses by using tried-and-true industry-tested and accepted methods for securing data.

Ensure proper configuration.

Encryption – even strong methods – won't protect your users if you don't configure it properly. That's one message businesses can take from the FTC's actions against ***Fandango*** and ***Credit Karma***. In those cases, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

5 Segment your network and monitor who's trying to get in and out.

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Segment your network.

Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network. That's a lesson from the ***DSW*** case. The FTC alleged that the company didn't sufficiently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks. The company could have reduced that risk by sufficiently segmenting its network.

Monitor activity on your network.

"Who's that knocking on my door?" That's what an effective intrusion detection tool asks when it detects unauthorized activity on your network. In the ***Dave & Buster's*** case, the FTC alleged that the company didn't use an intrusion detection system and didn't monitor system logs for suspicious activity. The FTC says something similar happened in ***Cardsystem Solutions***. The business didn't use sufficient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company's network that collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks.

6 Secure remote access to your network.

Business doesn't just happen in the office. While a mobile workforce can increase productivity, it also can pose new security challenges. If you give employees, clients, or service providers remote access to your network, have you taken steps to secure those access points? FTC cases suggest some factors to consider when developing your remote access policies.

Ensure endpoint security.

Just as a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it. That's the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For example, in ***Premier Capital Lending***, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business's security. When hackers accessed the client's system, they stole its remote login credentials and used them to grab consumers' personal information. According to the complaint in ***Settlement One***, the business allowed clients that didn't have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal. And in ***Lifelock***, the FTC charged that the company failed to install antivirus programs on the computers that employees used to remotely access its network. These businesses could have reduced those risks by securing computers that had remote access to their networks.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. That's why it's wise to limit access to what's needed to get the job done. In the ***Dave & Buster's*** case, for example, the FTC charged that the company failed to adequately restrict third-party access to its network. By exploiting security weaknesses in the third-party company's system, an intruder allegedly connected to the network numerous times and intercepted personal information. What could the company have done to reduce that risk? It could have placed limits on third-party access to its network – for example, by restricting connections to specified IP addresses or granting temporary, limited access.

7 Apply sound security practices when developing new products.

So you have a great new app or innovative software on the drawing board. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely? Before going to market, consider the lessons from FTC cases involving product development, design, testing, and roll-out.

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? In cases like ***MTS***, ***HTC America***, and ***TRENDnet***, the FTC alleged that the companies failed to train their employees in secure coding practices. The upshot: questionable design decisions, including the introduction of vulnerabilities into the software. For example, according to the complaint in ***HTC America***, the company failed to implement readily available secure communications mechanisms in the logging applications it pre-installed on its mobile devices. As a result, malicious third-party apps could communicate with the logging applications, placing consumers' text messages, location data, and other sensitive information at risk. The company could have reduced the risk of vulnerabilities like that by adequately training its engineers in secure coding practices.

Follow platform guidelines for security.

When it comes to security, there may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts. In actions against ***HTC America***, ***Fandango***, and ***Credit Karma***, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned off a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for developers, which explicitly warn against turning off SSL certificate validation.

Verify that privacy and security features work.

If your software offers a privacy or security feature, verify that the feature works as advertised. In ***TRENDnet***, for example, the FTC charged that the company failed to test that an option to make a consumer's camera feed private would, in fact, restrict access to that feed. As a result, hundreds of "private" camera feeds were publicly available. Similarly, in ***Snapchat***, the company advertised that messages would "disappear forever," but the FTC says it failed to ensure the accuracy of that claim. Among other things, the app saved video files to a location outside of the app's sandbox, making it easy to recover the video files with common file browsing tools. The lesson for other companies: When offering privacy and security features, ensure that your product lives up to your advertising claims.

Test for common vulnerabilities.

There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in the ***Guess?*** case, the FTC alleged that the business failed to assess whether its web application was vulnerable to Structured Query Language (SQL) injection attacks. As a result, hackers were able to use SQL attacks to gain access to databases with consumers' credit card information. That's a risk that could have been avoided by testing for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).

8 Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In ***GMR Transcription***, for example, the FTC alleged that the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed on the internet. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can't be a "take our word for it" thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process. The ***Upromise*** case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to "remove any personally identifiable information" before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted it in clear text. How could the company have reduced that risk? By asking questions and following up with the service provider during the development process.

9 Put procedures in place to keep your security current and address vulnerabilities that may arise.

Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up. If you use third-party software on your networks, or you include third-party software libraries in your applications, apply updates as they're issued. If you develop your own software, how will people let you know if they spot a vulnerability, and how will you make things right? FTC cases offer points to consider in thinking through vulnerability management.

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. In the ***TJX Companies*** case, for example, the FTC alleged that the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Depending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.

Heed credible security warnings and move quickly to fix them.

When vulnerabilities come to your attention, listen carefully and then get a move on. In the ***HTC America*** case, the FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions. Sometimes, companies receive security alerts, but they get lost in the shuffle. In ***Fandango***, for example, the company relied on its general customer service system to respond to warnings about security risks. According to the complaint, when a researcher contacted the business about a vulnerability, the system incorrectly categorized the report as a password reset request, sent an automated response, and marked the message as "resolved" without flagging it for further review. As a result, Fandango didn't learn about the vulnerability until FTC staff contacted the company. The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security@yourcompany.com) for receiving reports and flagging them for your security staff.

10 Secure paper, physical media, and devices.

Network security is a critical consideration, but many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives, and disks. FTC cases offer some things to consider when evaluating physical security at your business.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. In the ***Gregory Navone*** case, the FTC alleged that the defendant maintained sensitive consumer information, collected by his former businesses, in boxes in his garage. In ***Lifelock***, the complaint charged that the company left faxed documents that included consumers' personal information in an open and easily accessible area. In each case, the business could have reduced the risk to their customers by implementing policies to store documents securely.

Protect devices that process personal information.

Securing information stored on your network won't protect your customers if the data has already been stolen through the device that collects it. In the 2007 ***Dollar Tree*** investigation, FTC staff said that the business's PIN entry devices were vulnerable to tampering and theft. As a result, unauthorized persons could capture consumer's payment card data, including the magnetic stripe data and PIN, through an attack known as "PED skimming." Given the novelty of this type of attack at the time, and a number of other factors, staff closed the investigation. However, attacks targeting point-of-sale devices are now common and well-known, and businesses should take reasonable steps to protect such devices from compromise.

Keep safety standards in place when data is en route.

Savvy businesses understand the importance of securing sensitive information when it's outside the office. In ***Accretive***, for example, the FTC alleged that an employee left a laptop containing more than 600 files, with 20 million pieces of information related to 23,000 patients, in the locked passenger compartment of a car, which was then stolen. The ***CBR Systems*** case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive – all of which contained sensitive information – that were lifted from an employee's car. In each case, the business could have reduced the risk to consumers' personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets you track where the package is. Limit the instances when employees need to be out and about with sensitive data in their possession. But when there's a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.

Dispose of sensitive data securely.

Paperwork or equipment you no longer need may look like trash, but it's treasure to identity thieves if it includes personal information about consumers or employees. For example, according to the FTC complaints in ***Rite Aid*** and ***CVS Caremark***, the companies tossed sensitive personal information – like prescriptions – in dumpsters. In ***Goal Financial***, the FTC alleged that an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The companies could have prevented the risk to consumers' personal information by shredding, burning, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

Looking for more information?

The FTC's Business Center (**business.ftc.gov**) has a Data Security section with an up-to-date listing of relevant cases and other free resources.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at **business.ftc.gov**.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman.**

Federal Trade Commission
business.ftc.gov
June 2015

PENNSYLVANIA BAR ASSOCIATION COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/ SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY

FORMAL OPINION 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer." [1]

From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs.

This opinion places all such software and services under the "cloud computing" label, as each raises essentially the same ethical issues. In particular, the central question posed by "cloud computing" may be summarized as follows:

> May an attorney ethically store confidential client material in "the cloud"?

In response to this question, this Committee concludes:

> Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

****

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

[1] Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than "cloud computing," which refers to software and related services that store information on a remote computer, *i.e.*, a computer or server that is not located at the law office's physical location. Rather, the information is stored on another company's server, or many servers, possibly all over the world, and the user's computer becomes just a way of accessing the information.[2]

The advent of "cloud computing," as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in "cloud computing."

Recent "cloud" data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission ("FTC") has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of "cloud computing" and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations ("FBI") warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms' databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 ("Metadata") and 2010-200 ("Virtual Law Offices"), and an informal Opinion directly addressing "cloud computing." Because of the importance of "cloud computing" to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing "cloud computing."

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.*, products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

II. Background

For lawyers, "cloud computing" may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with "cloud computing," an attorney can simplify document management and control costs.

[2] *Id.*

The benefits of using "cloud computing" may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because "cloud computing" refers to "offsite" storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

III. Discussion

A. Prior Pennsylvania Opinions

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office "is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office." Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on "cloud computing" stated that an attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

B. Pennsylvania Rules of Professional Conduct

An attorney using "cloud computing" is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses "cloud computing," the following rules, *inter alia,* are implicated:

> Rule 1.0 ("Terminology");
> Rule 1.1 ("Competence");
> Rule 1.4 ("Communication");
> Rule 1.6 ("Confidentiality of Information");
> Rule 1.15 ("Safekeeping Property"); and
> Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants").

Rule 1.1 ("Competence") states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [5] ("Thoroughness and Preparation") of Rule 1.1 provides further guidance about an attorney's obligations to clients that extend beyond legal skills:

> Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. …

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney's "methods and procedures." Part of a lawyer's responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like "cloud computing," require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in "cloud computing" is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children's show "Zodiac Island" lost an entire season's worth of episodes when a fired employee for the show's data hosting service accessed the show's content without authorization and wiped it out.[3]

[3] Eriq Gardner, "Hacker Erased a Season's Worth of 'Zodiac Island'," *Yahoo! TV* (March 31, 2011), available at http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac

Rule 1.15 ("Safekeeping Property") requires that client property should be "appropriately safeguarded."[4] Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

> (b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer's own property. Such property shall be identified and appropriately safeguarded.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> (d) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

> A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. …

Also relevant is Rule 1.0(e) defining the requisite "Informed Consent":

> "Informed consent" denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client's informed consent is required. While it is not necessary to communicate every minute

[4] In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the "cloud."

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).[5] This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

> 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. This duty, however, 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 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.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

[5] The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using "cloud computing" services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.[6]

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants") states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) A partner 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 the person's conduct is compatible with the professional obligations of the lawyer.
>
> (b) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

At its essence, "cloud computing" can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client's interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client's matter.

C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider

[6] Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of "cloud computing," an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney's direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. Competency extends beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider. However, since cloud services are under the provider's control, using "the cloud" to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;

- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;
    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
    - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
    - provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.

- Investigating the provider's:
    - security measures, policies and recovery methods;
    - system for backing up data;
    - security of data centers and whether the storage is in multiple centers;
    - safeguards against disasters, including different server locations;
    - history, including how long the provider has been in business;
    - funding and stability;
    - policies for data retrieval upon termination of the relationship and any related charges; and,
    - process to comply with data that is subject to a litigation hold.

- Determining whether:
    - data is in non-proprietary format;
    - the Service Level Agreement clearly states that the attorney owns the data;
    - there is a 3rd party audit of security; and,
    - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.[7]

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the "cloud computing" services are offered, *i.e.*, Service Level Agreements ("SLAs"), may also present obstacles to reasonable care efforts. Most SLAs are essentially "take it or leave it,"[8] and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the "cloud computing" field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.[9]

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania's notification law, 73 P.S. § 2303 (2011) ("Notification of Breach"), states:

> (a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
>
> (b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

---

[7] This is recommended even though many vendors will claim that it is not necessary.

[8] Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

[9] One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

> (c) VENDOR NOTIFICATION. -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for "cloud computing." In the survey, a number of the nearly 900 internet experts surveyed agreed that it "presents security problems and further exposes private information," and some experts even predicted that "the cloud" will eventually have a massive breach from cyber-attacks.[10] Incident response plans should be in place before attorneys move to "the cloud", and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be "private clouds." Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

D. Web-based E-mail

Web-based email ("webmail") is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of "cloud computing," are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney's obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, "Legal Ethics in the Cloud: Avoiding the Storms," explains:

> Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

[10] Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all

> these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.[11]

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

> In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.
>
> It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.[12]

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) ("Transmission of Confidential Information by Electronic Mail"), which concluded that, "In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security."

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 ("Confidentiality of Information").

> Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate's law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm's mail room if that message contained client confidential

[11] David G. Ries, Esquire, "Legal Ethics in the Cloud: Avoiding the Storms," course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).
[12] *Id*.

information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.

By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

E. Opinions From Other Ethics Committees

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while "cloud computing" is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.,* web-based email) and these conclusions are consistent with opinions about emergent emergent "cloud computing" technologies.

The American Bar Association Standing Committee on Ethics and Professional Responsibility has not yet issued a formal opinion on "cloud computing." However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" (Sept. 20, 2010) and considered some of the concerns and ethical implications of using "the cloud." The Working Group found that potential confidentiality problems involved with "cloud computing" include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

Id. The Working Group also stated, "[f]orms of technology other than 'cloud computing' can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen." *Id*. Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

Id. Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 ("Terminology"), Model Rule 1.1 ("Competence"), and Model Rule 1.6 ("Duty of Confidentiality") to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

> Rule 1.1 ("Competence") Comment [6] ("Maintaining Competence"): "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 technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
>
> Rule 1.6(c) ("Duty of Confidentiality"): "A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."
>
> Rule 1.6 ("Duty of Confidentiality") Comment [16] ("Acting Competently to Preserve Confidentiality"): "Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

> be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id*.

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

The Alabama State Bar Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

State Bar of Arizona Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id*. Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

The California State Bar Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

The Florida Bar Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id*.

Illinois State Bar Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."[13]

The Maine Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id*.

Of note, the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provide a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

> The contract between a covered entity and a business associate must provide that the business associate will:
>
> (A) 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 covered entity as required by this subpart;

[13] Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) 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.

Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id*.

The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id*. Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

The New Jersey State Bar Association Advisory Committee on Professional Ethics issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id*. Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id*. The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

The New York State Bar Association Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against "reasonably foreseeable" data infiltration by using available technology. *Id*.

The North Carolina State Bar Ethics Committee has addressed the issue of "cloud computing" directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that "a law firm may use SaaS[14] if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files." *Id*. The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers "must protect against security weaknesses unique to the Internet, particularly 'end-user' vulnerabilities found in the lawyer's own law office." *Id*.

The Committee's minimum requirements for reasonable care in Proposed Formal Opinion 6 included:[15]

- An agreement on how confidential client information will be handled in keeping with the lawyer's professional responsibilities must be included in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;

- The agreement with the vendor must specify that firm's data will be hosted only within a specified geographic area. If by agreement the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the state of North Carolina;

- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor's software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

[14] SaaS, as stated above, stands for Software-as-a-Service and is a type of "cloud computing."

[15] The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, "due diligence and perpetual education as to the security risks of SaaS are required." Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data "off" the vendor's or third party data hosting company's servers for lawyers' own use or in-house backup offline; and,

- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

Vermont Bar Association Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)[16], requiring "due care" in selecting the service provider and keeping the information confidential. *Id*.

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

IV. Conclusion

The use of "cloud computing," and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

[16] Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

> To the extent a lawyer reasonably believes necessary, the lawyer may reveal:
>
> (6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in "the cloud." Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using "cloud" software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.1

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

History

SOURCE:

The provisions of this Rule 1.1 amended October 22, 2013, effective in 30 days, *43 Pa.B. 6641.* Immediately preceding text appears at serial pages (309395) to (309396).

Annotations

Notes

NOTES:

Commentary

Comment:

Legal Knowledge and Skill

(1) In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

(2) A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

(3) In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impracticable. Even in an emergency,

however, assistance should be limited to that reasonably necessary in the circumstances, for ill considered action under emergency conditions can jeopardize the client's interest.

(4) A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

(5) Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may limit the matters for which the lawyer is responsible. See Rule 1.2(c).

Retaining or Contracting With Other Lawyers

(6) Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. See also Rules 1.2, 1.4, 1.6, and 5.5(a). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the education, experience and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

(7) When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

(8) 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.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.4

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.4. Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

(c) A lawyer in private practice shall inform a new client in writing if the lawyer does not have professional liability insurance of at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year, subject to commercially reasonable deductibles, retention or co-insurance, and shall inform existing clients in writing at any time the lawyer's professional liability insurance drops below either of those amounts or the lawyer's professional liability insurance is terminated. A lawyer shall maintain a record of these disclosures for six years after the termination of the representation of a client.

History

SOURCE:

The provisions of this Rule 1.4 amended October 22, 2013, effective in 30 days, *43 Pa.B. 6641.* Immediately preceding text appears at serial pages (316365) to (316367).

Annotations

Notes

NOTES:

Commentary

Comment:

(1) Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

Communicating with Client

(2) If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

(3) Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations -- depending on both the importance of the action under consideration and the feasibility of consulting with the client -- this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

(4) A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

Explaining Matters

(5) The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(e).

(6) Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

(7) In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interests or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client.

Disclosures Regarding Insurance

(8) Paragraph (c) does not apply to lawyers in full-time government practice or full-time lawyers employed as in-house counsel and who do not have any private clients.

(9) Lawyers may use the following language in making the disclosures required by this rule:

(i) No insurance or insurance below required amounts when retained: "*Pennsylvania Rule of Professional Conduct 1.4(c)* requires that you, as the client, be informed in writing if a lawyer does not have professional liability insurance of at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year and if, at any time, a lawyer's professional liability insurance drops below either of those amounts or a lawyer's professional liability insurance coverage is terminated. You are therefore advised that (name of attorney or firm) does not have professional liability insurance coverage of at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year."

(ii) Insurance drops below required amounts: "*Pennsylvania Rule of Professional Conduct 1.4(c)* requires that you, as the client, be informed in writing if a lawyer does not have professional liability insurance of at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year and if, at any time, a lawyer's professional liability insurance drops below either of those amounts or a lawyer's professional liability insurance coverage is terminated. You are therefore advised that (name of attorney or firm)'s professional liability insurance dropped below at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year as of (date)."

(iii) Insurance terminated: "*Pennsylvania Rule of Professional Conduct 1.4(c)* requires that you, as the client, be informed in writing if a lawyer does not have professional liability insurance of at least $ 100,000 per occurrence and $ 300,000 in the aggregate per year and if, at any time, a lawyer's professional liability insurance drops below either of those amounts or a lawyer's professional liability insurance coverage is terminated. You are therefore advised that (name of attorney or firm)'s professional liability insurance has been terminated as of (date)."

(10) A lawyer or firm maintaining professional liability insurance coverage in at least the minimum amounts provided in paragraph (c) is not subject to the disclosure obligations mandated by the rule if such coverage is subject to commercially reasonable deductibles, retention or co-insurance. Deductibles, retentions or co-insurance offered, from time to time, in the marketplace for professional liability insurance for the size of firm and coverage limits purchased will be deemed to be commercially reasonable.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.6

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.6. Confidentiality of Information

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).

(b) A lawyer shall reveal such information if necessary to comply with the duties stated in Rule 3.3.

(c) A lawyer may reveal such information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a criminal act that the lawyer believes is likely to result in substantial injury to the financial interests or property of another;

(3) to prevent, mitigate or rectify the consequences of a client's criminal or fraudulent act in the commission of which the lawyer's services are being or had been used; or

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim or disciplinary proceeding against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(5) to secure legal advice about the lawyer's compliance with these Rules; or

(6) to effectuate the sale of a law practice consistent with Rule 1.17; or

(7) to detect and resolve conflicts of interest from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(d) 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.

(e) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

History

SOURCE:

The provisions of this Rule 1.6 amended May 17, 2012, effective in 30 days, *42 Pa.B. 3127;* amended October 22, 2013, effective in 30 days, *43 Pa.B. 6641.* Immediately preceding text appears at serial pages (316369), (309403) to (309404) and (361481) to (361482).

Annotations

Notes

NOTES:

Commentary

Comment:

(1) This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

(2) A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communi-cate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

(3) The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work-product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.

(4) Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

(5) A lawyer has duties of disclosure to a tribunal under Rule 3.3(a) that may entail disclosure of information relating to the representation. Rule 1.6(b) recognizes the paramount nature of this obligation.

Authorized Disclosure

(6) Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation . In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

Detection of Conflicts of Interest

(7) Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. In becoming

privy to information about a client, a lawyer may foresee that the client intends or learn that the client has caused serious harm to another person. However, to the extent that a lawyer is required or permitted to disclose a client's purposes or conduct, the client may be inhibited from revealing facts that would enable the lawyer effectively to represent the client. Generally, the public interest is better served if full disclosure by clients to their lawyers is encouraged rather than inhibited. With limited exceptions, information relating to the representation must be kept confidential by a lawyer, as stated in paragraph (a).

(8) Where human life is threatened, the client is or has been engaged in criminal or fraudulent conduct, or the integrity of the lawyer's own conduct is involved, the principle of confidentiality may have to yield, depending on the lawyer's knowledge about and relationship to the conduct in question.

(9) Several situations must be distinguished:

(10) First, a lawyer may foresee certain death or serious bodily harm to another person. Paragraph (c)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and that the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims.

(11) Second, paragraph (c)(2) is a limited exception to the rule of confidentiality that permits the lawyer to reveal information to the extent necessary to enable affected persons or appropriate authorities to prevent the client from committing a crime that is reasonably certain to result in substantial injury to the financial or property interests of another. Disclosure is permitted under paragraph (c)(2) only where the lawyer reasonably believes that such threatened action is a crime; the lawyer may not substitute his or her own sense of wrongdoing for that of society at large as reflected in the applicable criminal laws. The client can, of course, prevent such disclosure by refraining from the wrongful conduct.

(12) Third, a lawyer may not counsel or assist a client in conduct that is criminal or fraudulent. See Rule 1.2(d). To avoid assisting a client's criminal or fraudulent conduct, the lawyer may have to reveal information relating to the representation. Rule 1.6(c)[(2)](3) permits doing so.

(13) Fourth, a lawyer may have been innocently involved in past conduct by a client that was criminal or fraudulent. In such a situation, the lawyer did not violate Rule 1.2(d). However, if the lawyer's services were made an instrument of the client's crime or fraud, the lawyer has a legitimate and overriding interest in being able to rectify the consequences of such conduct. Rule 1.6(c)(3) gives the lawyer professional discretion to reveal information relating to the representation to the extent necessary to accomplish rectification.

(14) Fifth, where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person; for example, a person claiming to have been defrauded by the lawyer and client acting together. If the lawyer is charged with wrongdoing in which the client's conduct is implicated, the rule of confidentiality should not prevent the lawyer from defending against the charge. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (c)(4) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

(15) Sixth, a lawyer entitled to a fee is permitted by paragraph (c)(4) to prove the services rendered in an action to collect it. This aspect of the Rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

(16) Seventh, a lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (c)(5) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

(17) Eighth, it is recognized that the due diligence associated with the sale of a law practice authorized under Rule 1.17 may necessitate the limited disclosure of certain otherwise confidential information. Paragraph (c)(6) permits such disclosure. However, as stated above, the lawyer must make every effort practicable to avoid unnecessary disclosure of information relating to a representation, to limit disclosure to those having a need to know it, and to obtain appropriate arrangements minimizing the risk of disclosure.

(18) Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4.

(19) Paragraph (c)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment (4). Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any such disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. Moreover, the disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these Rules.

(20) Any information disclosed pursuant to paragraph (c)(7) may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. Paragraph (c)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (c)(7). Paragraph (c)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment (6), such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

(21) A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4.

(22) Paragraph (c) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

(23) Paragraph (c) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (c)(1) through (c)(7). In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (c) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (c). See Rules 1.2(d), 4.1(b), 8.1 and 8.3. Rule 3.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).

Withdrawal

(24) If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw, as stated in Rule 1.16(a)(1). After withdrawal the lawyer is required to refrain from making disclosure of the client's confidences, except as otherwise provided in Rule 1.6. Neither this Rule nor Rule 1.8(b) nor Rule 1.16(d) prevents the lawyer from giving notice of the fact of withdrawal, and the lawyer may also withdraw or disaffirm any opinion, document, affirmation, or the like. Where the client is an organization, the lawyer may be in doubt whether contemplated conduct will actually be carried out by the organization. Where necessary to guide conduct in connection with this Rule, the lawyer may make inquiry within the organization as indicated in Rule 1.13(b).

Acting Competently to Preserve Confidentiality

(25) Paragraph (d) 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 (d) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments (3) -- (4).

(26) 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. This duty, however, 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 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Former Client

(27) The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.

Lobbyists

(28) A lawyer who acts as a lobbyist on behalf of a client may disclose information relating to the representation in order to comply with any legal obligation imposed on the lawyer-lobbyist by the Legislature, the Executive Branch or an agency of the Commonwealth, or a local government unit which are consistent with the Rules of Professional Conduct. Such disclosure is explicitly authorized to carry out the representation. The Disciplinary Board of the Supreme Court shall retain jurisdiction over any violation of this Rule.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.9

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.9. Duties to Former Clients

(a) A lawyer who has formerly represented a client in a matter shall not thereafter represent another person in the same or a substantially related matter in which that person's interests are materially adverse to the interests of the former client unless the former client gives informed consent.

(b) A lawyer shall not knowingly represent a person in the same or a substantially related matter in which a firm with which the lawyer formerly was associated had previously represented a client

(1) whose interests are materially adverse to that person; and

(2) about whom the lawyer had acquired information protected by Rules 1.6 and 1.9(c) that is material to the matter;

unless the former client gives informed consent.

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:

(1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or

(2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.

Annotations

Notes

NOTES:

Commentary

Comment:

(1) After termination of a client-lawyer relationship, a lawyer has certain continuing duties with respect to confidentiality and conflicts of interest and thus may not represent another client except in conformity with this Rule. Under this Rule, for example, a lawyer could not properly seek to rescind on behalf of a new client a contract drafted on behalf of the former client. So also a lawyer who has prosecuted an accused person could not properly represent the accused in a subsequent civil action against the government concerning the same transaction. Nor could a lawyer who has represented multiple clients in a matter represent one of the clients against the others in the same or a substantially related matter after a dispute arose among the clients in that matter, unless all affected clients give informed consent. See Comment (9). Current and former government lawyers must comply with this Rule to the extent required by Rule 1.11.

(2) The scope of a "matter" for purposes of this Rule depends on the facts of a particular situation or transaction. The lawyer's involvement in a matter can also be a question of degree. When a lawyer has been directly involved in a specific transaction,

subsequent representation of other clients with materially adverse interests in that transaction clearly is prohibited. On the other hand, a lawyer who recurrently handled a type of problem for a former client is not precluded from later representing another client in a factually distinct problem of that type even though the subsequent representation involves a position adverse to the prior client. Similar considerations can apply to the reassignment of military lawyers between defense and prosecution functions within the same military jurisdictions. The underlying question is whether the lawyer was so involved in the matter that the subsequent representation can be justly regarded as a changing of sides in the matter in question.

(3) Matters are "substantially related" for purposes of this Rule if they involve the same transaction or legal dispute or if there otherwise is a substantial risk that confidential factual information as would normally have been obtained in the prior representation would materially advance the client's position in the subsequent matter. For example, a lawyer who has represented a businessperson and learned extensive private financial information about that person may not then represent that person's spouse in seeking a divorce. Similarly, a lawyer who has previously represented a client in securing environmental permits to build a shopping center would be precluded from representing neighbors seeking to oppose rezoning of the property on the basis of environmental considerations; however, the lawyer would not be precluded, on the grounds of substantial relationship, from defending a tenant of the completed shopping center in resisting eviction for nonpayment of rent. Information that has been disclosed to the public or to other parties adverse to the former client ordinarily will not be disqualifying. Information acquired in a prior representation may have been rendered obsolete by the passage of time, a circumstance that may be relevant in determining whether two representations are substantially related. In the case of an organizational client, general knowledge of the client's policies and practices ordinarily will not preclude a subsequent representation; on the other hand, knowledge of specific facts gained in a prior representation that are relevant to the matter in question ordinarily will preclude such a representation. A former client is not required to reveal the confidential information learned by the lawyer in order to establish a substantial risk that the lawyer has confidential information that could be used adversely to the former client's interests in the subsequent matter. A conclusion about the possession of such information may be based on the nature of the services the lawyer provided the former client and information that would in ordinary practice be learned by a lawyer providing such services.

Lawyers Moving Between Firms

(4) When lawyers have been associated with a firm but then end their association, the question of whether a lawyer should undertake representation is more complicated. There are several competing considerations. First, the client previously represented by the former firm must be reasonably assured that the principle of loyalty to the client is not compromised. Second, the Rule should not be so broadly cast as to preclude other persons from having reasonable choice of legal counsel. Third, the Rule should not unreasonably hamper lawyers from forming new associations and taking on new clients after having left a previous association. In this connection, it should be recognized that today many lawyers practice in firms, that many lawyers to some degree limit their practice to one field or another, and that many move from one association to another several times in their careers. If the concept of imputation were applied with unqualified rigor, the result would be radical curtailment of the opportunity of lawyers to move from one practice setting to another and of the opportunity of clients to change counsel.

(5) Paragraph (b) operates to disqualify the lawyer only when the lawyer involved has actual knowledge information protected by Rules 1.6 and 1.9(c). Thus, if a lawyer while with one firm acquired no knowledge of information relating to a particular client of the firm, and that lawyer later joined another firm, neither the lawyer individually nor the second firm is disqualified from representing another client in the same or a related matter even though the interests of the two clients conflict. See Rule 1.10(b) for the restrictions on a firm once a lawyer becomes associated with a firm, including screening provisions. See Rule 1.10(c) for the restrictions on a firm once a lawyer has terminated association with the firm.

(6) Application of paragraph (b) depends on a situation's particular facts, aided by inferences, deductions or working presumptions that reasonably may be made about the way in which lawyers work together. A lawyer may have general access to files of all clients of a law firm and may regularly participate in discussions of their affairs; it should be inferred that such a lawyer in fact is privy to all information about all the firm's clients. In contrast, another lawyer may have access to the files of only a limited number of clients and participate in discussions of the affairs of no other clients; in the absence of information to the contrary, it should be inferred that such a lawyer in fact is privy to information about the clients actually served but not those of other clients. In such an inquiry, the burden of proof should rest upon the firm whose disqualification is sought.

(7) Independent of the question of disqualification of a firm, a lawyer changing professional association has a continuing duty to preserve confidentiality of information about a client formerly represented. See Rules 1.6 and 1.9(c).

(8) Paragraph (c) provides that information acquired by the lawyer in the course of representing a client may not subsequently be used or revealed by the lawyer to the disadvantage of the client. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client when later representing another client.

(9) The provisions of this Rule are for the protection of former clients and can be waived if the client gives informed consent. See Rule 1.0 (e). With regard to the effectiveness of an advance waiver, see Comment (22) to Rule 1.7. With regard to disqualification of a firm with which a lawyer is or was formerly associated, see Rule 1.10.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.15

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.15. Safekeeping Property

(a) The following definitions are applicable to Rule 1.15:

(1) Eligible Institution. An Eligible Institution is a Financial Institution which has been approved as a depository of Trust Accounts pursuant to Pa.R.D.E. 221(h).

(2) Fiduciary. A Fiduciary is a lawyer acting as a personal representative, guardian, conservator, receiver, trustee, agent under a durable power of attorney, or other similar position.

(3) Fiduciary Funds. Fiduciary Funds are Rule 1.15 Funds which the lawyer holds as a Fiduciary. Fiduciary Funds may be either Qualified Funds or Nonqualified Funds.

(4) Financial Institution. A Financial Institution is an entity which is authorized by federal or state law and licensed to do business in the Commonwealth of Pennsylvania as one of the following: a bank, bank and trust company, trust company, credit union, savings bank, savings and loan association or foreign banking corporation, the deposits of which are insured by an agency of the federal government, or as an investment adviser registered under the Investment Advisers Act of 1940 or with the Pennsylvania Securities Commission, an investment company registered under the Investment Company Act of 1940, or a broker dealer registered under the Securities Exchange Act of 1934.

(5) Interest On Lawyer Trust Account (IOLTA) Account. An IOLTA Account is an income producing Trust Account from which funds may be withdrawn upon request as soon as permitted by law. Qualified Funds are to be held or deposited in an IOLTA Account.

(6) IOLTA Board. The IOLTA Board is the Pennsylvania Interest On Lawyers Trust Account Board.

(7) Non-IOLTA Account. A Non-IOLTA Account is an income producing Trust Account from which funds may be withdrawn upon request as soon as permitted by law in which a lawyer deposits Rule 1.15 Funds. Only Nonqualified Funds are to be held or deposited in a Non-IOLTA Account. A Non-IOLTA Account shall be established only as:

(i) a separate client Trust Account for the particular client or matter on which the net income will be paid to the client or third person; or

(ii) a pooled client Trust Account with subaccounting by the Eligible Institution or by the lawyer, which will provide for computation of net income earned by each client's or third person's funds and the payment thereof to the client or third person.

(8) Nonqualified Funds. Nonqualified Funds are Rule 1.15 Funds, whether cash, check, money order or other negotiable instrument, which are not Qualified Funds.

(9) Qualified Funds. Qualified Funds are Rule 1.15 Funds which are nominal in amount or are reasonably expected to be held for such a short period of time that sufficient income will not be generated to justify the expense of administering a segregated account.

(10) Rule 1.15 Funds. Rule 1.15 Funds are funds which the lawyer receives from a client or third person in connection with a client-lawyer relationship, or as an escrow agent, settlement agent or representative payee, or as a Fiduciary, or receives as an agent, having been designated as such by a client or having been so selected as a result of a client-lawyer relationship or the lawyer's status as such. When the term "property" appears with "Rule 1.15 Funds," it means property of a client or third person which the lawyer receives in any of the foregoing capacities.

(11) Trust Account. A Trust Account is an account in an Eligible Institution in which a lawyer holds Rule 1.15 Funds. A Trust Account must be maintained either as an IOLTA Account or as a Non-IOLTA Account.

(b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer's own property. Such property shall be identified and appropriately safeguarded.

(c) Required records. Complete records of the receipt, maintenance and disposition of Rule 1.15 Funds and property shall be preserved for a period of five years after termination of the client-lawyer or Fiduciary relationship or after distribution or disposition of the property, whichever is later. A lawyer shall maintain the writing required by Rule 1.5(b) (relating to the requirement of a writing communicating the basis or rate of the fee) and the records identified in Rule 1.5(c) (relating to the requirement of a written fee agreement and distribution statement in a contingent fee matter). A lawyer shall also maintain the following books and records for each Trust Account and for any other account in which Fiduciary Funds are held pursuant to Rule 1.15(l):

(1) all transaction records provided to the lawyer by the Financial Institution or other investment entity, such as periodic statements, cancelled checks in whatever form, deposited items and records of electronic transactions; and

(2) check register or separately maintained ledger, which shall include the payee, date, purpose and amount of each check, withdrawal and transfer, the payor, date, and amount of each deposit, and the matter involved for each transaction; provided, however, that where an account is used to hold funds of more than one client, a lawyer shall also maintain an individual ledger for each trust client, showing the source, amount and nature of all funds received from or on behalf of the client, the description and amounts of charges or withdrawals, the names of all persons or entities to whom such funds were disbursed, and the dates of all deposits, transfers, withdrawals and disbursements.

(3) The records required by this Rule may be maintained in hard copy form or by electronic, photographic, or other media provided that the records otherwise comply with this Rule and that printed copies can be produced. Whatever method is used to maintain required records must have a backup so that the records are secure and always available. If records are kept only in electronic form, then such records shall be backed up on a separate electronic storage device at least at the end of any day on which entries have been entered into the records. These records shall be readily accessible to the lawyer and available for production to the Pennsylvania Lawyers Fund for Client Security or the Office of Disciplinary Counsel in a timely manner upon a request or demand by either agency made pursuant to the Pennsylvania Rules of Disciplinary Enforcement, the Disciplinary Board Rules, the Pennsylvania Lawyers Fund for Client Security Board Rules and Regulations, agency practice, or subpoena.

(4) A regular trial balance of the individual client trust ledgers shall be maintained. The total of the trial balance must agree with the control figure computed by taking the beginning balance, adding the total of moneys received in trust for the client, and deducting the total of all moneys disbursed. On a monthly basis, a lawyer shall conduct a reconciliation for each fiduciary account. The reconciliation is not complete if the reconciled total cash balance does not agree with the total of the client balance listing. A lawyer shall preserve for a period of five years copies of all records and computations sufficient to prove compliance with this requirement.

(d) Upon receiving Rule 1.15 Funds or property which are not Fiduciary Funds or property, a lawyer shall promptly notify the client or third person, consistent with the requirements of applicable law. Notification of receipt of Fiduciary Funds or property to clients or other persons with a beneficial interest in such Fiduciary Funds or property shall continue to be governed by the law, procedure and rules governing the requirements of confidentiality and notice applicable to the Fiduciary entrustment.

(e) Except as stated in this Rule or otherwise permitted by law or by agreement with the client or third person, a lawyer shall promptly deliver to the client or third person any property, including but not limited to Rule 1.15 Funds, that the

client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding the property; Provided, however, that the delivery, accounting and disclosure of Fiduciary Funds or property shall continue to be governed by the law, procedure and rules governing the requirements of Fiduciary administration, confidentiality, notice and accounting applicable to the Fiduciary entrustment.

(f) When in possession of funds or property in which two or more persons, one of whom may be the lawyer, claim an interest, the funds or property shall be kept separate by the lawyer until the dispute is resolved. The lawyer shall promptly distribute all portions of the funds or property, including Rule 1.15 Funds, as to which the interests are not in dispute.

(g) The responsibility for identifying an account as a Trust Account shall be that of the lawyer in whose name the account is held. Only a lawyer admitted to practice law in this jurisdiction or a person under the direct supervision of the lawyer shall be an authorized signatory or authorize transfers from a Trust Account or any other account in which Fiduciary Funds are held pursuant to Rule 1.15(l).

(h) A lawyer shall not deposit the lawyer's own funds in a Trust Account except for the sole purpose of paying service charges on that account, and only in an amount necessary for that purpose.

(i) A lawyer shall deposit into a Trust Account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred, unless the client gives informed consent, confirmed in writing, to the handling of fees and expenses in a different manner.

(j) At all times while a lawyer holds Rule 1.15 Funds, the lawyer shall also maintain another account that is not used to hold such funds.

(k) All Nonqualified Funds which are not Fiduciary Funds shall be placed in a Non-IOLTA Account or in another investment vehicle specifically agreed upon by the lawyer and the client or third person which owns the funds.

(l) All Fiduciary Funds shall be placed in a Trust Account (which, if the Fiduciary Funds are also Qualified Funds, must be an IOLTA Account) or in another investment or account which is authorized by the law applicable to the entrustment or the terms of the instrument governing the Fiduciary Funds.

(m) All Qualified Funds which are not Fiduciary Funds shall be placed in an IOLTA Account.

(n) A lawyer shall be exempt from the requirement that all Qualified Funds be placed in an IOLTA Account only upon exemption requested and granted by the IOLTA Board. If an exemption is granted, the lawyer must hold Qualified Funds in a Trust Account which is not income producing. Exemptions shall be granted if:

(1) the nature of the lawyer's practice does not require the routine maintenance of a Trust Account in Pennsylvania;

(2) compliance with this paragraph would work an undue hardship on the lawyer or would be extremely impractical, based either on the geographical distance between the lawyer's principal office and the closest Eligible Institution, or on other compelling and necessitous factors; or

(3) the lawyer's historical annual Trust Account experience, based on information from the Eligible Institution in which the lawyer deposits funds, demonstrates that the service charges on the account would significantly and routinely exceed any income generated.

(o) An account shall not be considered an IOLTA Account unless the Eligible Institution at which the account is maintained shall:

(1) Remit at least quarterly any income earned on the account to the IOLTA Board;

(2) Transmit to the IOLTA Board with each remittance and to the lawyer who maintains the IOLTA Account a statement showing at least the name of the account, service charges or fees deducted, if any, the amount of income remitted from the account, and the average daily balance, if available; and

(3) Pay a rate of interest or dividends no less than the highest interest rate or dividend generally available from the Eligible Institution to its Non-IOLTA customers when the IOLTA Account meets the same minimum balance or other eligibility qualifications, and comply with the Regulations of the IOLTA Board with respect to service charges, if any.

(p) A lawyer shall not be liable in damages or held to have breached any fiduciary duty or responsibility because monies are deposited in an IOLTA Account pursuant to the lawyer's judgment in good faith that the monies deposited were Qualified Funds.

(q) There is hereby created the Pennsylvania Interest On Lawyers Trust Account Board, which shall administer the IOLTA program. The IOLTA Board shall consist of nine members who shall be appointed by the Supreme Court. Two of the appointments shall be made from a list provided to the Supreme Court by the Pennsylvania Bar Association in accordance with its own rules and regulations. With respect to these two appointments, the Pennsylvania Bar Association shall submit three names to the Supreme Court, from which the Court shall make its final selections. The term of each member shall be three years and no member shall be appointed for more than two consecutive three year terms. The Supreme Court shall appoint a Chairperson. In order to administer the IOLTA program, the IOLTA Board shall promulgate rules and regulations consistent with this Rule for approval by the Supreme Court.

(r) The IOLTA Board shall comply with the following:

(1) The IOLTA Board shall prepare an annual audited statement of its financial affairs.

(2) The IOLTA Board shall submit to the Supreme Court for its approval a copy of its audited statement of financial affairs, clearly setting forth in detail all funds previously approved for disbursement under the IOLTA program and the IOLTA Board's proposed annual budget, designating the uses to which IOLTA Funds are recommended.

(3) Upon approval of the Supreme Court, the IOLTA Board shall distribute and/or expend IOLTA Funds.

(s) Income earned on IOLTA Accounts (IOLTA Funds) may be used only for the following purposes:

(1) delivery of civil legal assistance to the poor and disadvantaged in Pennsylvania by non-profit corporations described in section 501(c)(3) of the Internal Revenue Code of 1986, as amended;

(2) educational legal clinical programs and internships administered by law schools located in Pennsylvania;

(3) administration and development of the IOLTA program in Pennsylvania; and

(4) the administration of justice in Pennsylvania.

(t) The IOLTA Board shall hold the beneficial interest in IOLTA Funds. Monies received in the IOLTA program are not state or federal funds and are not subject to Article VI of the act of April 9, 1929 (P. L. 177, No. 175) known as The Administrative Code of 1929, or the act of June 29, 1976 (P. L. 469, No. 117).

(u) Every attorney who is required to pay an active annual assessment under Rule 219 of the Pennsylvania Rules of Disciplinary Enforcement (relating to annual registration of attorneys) shall pay an additional annual fee of $ 30.00 for use by the IOLTA Board. Such additional assessment shall be added to, and collected with and in the same manner as, the basic annual assessment. All amounts received pursuant to this subdivision shall be credited to the IOLTA Board.

History

SOURCE:

The provisions of this Rule 1.15 amended September 4, 2008, effective September 20, 2008, *38 Pa.B. 5157;* amended April 2, 2009, effective immediately, *39 Pa.B. 1980;* amended April 9, 2012 for the 2012-13 assessment and thereafter shall revert to the provisions effective for the 2011-12 assessment, effective immediately, *42 Pa.B. 2186;* amended June 4, 2012, effective in 30 days, *42 Pa.B. 3431;* under the order of February 12, 2013, the order of April 9, 2012 amending subsection (u) shall remain in effect for the 2013-14 annual attorney assessment and in one year shall revert to the provisions effective on April 8, 2012, effective immediately, *43 Pa.B. 1173;* amended May 1, 2014, effective immediately for the 2014-15 annual attorney assessment and shall continue until further Order of the Supreme Court, *44 Pa.B. 2847;* amended December 30, 2014, effective in 60 days, *45 Pa.B. 279;* amended February 9, 2015, effective immediately, *45 Pa.B. 953.* Immediately preceding text appears at serial pages (342518) and (376189) to (376195).

Annotations

Notes

NOTES:

Commentary

Comment:

(1) A lawyer should hold property of others with the care required of a professional fiduciary. The obligations of a lawyer under this Rule apply when the lawyer has come into possession of property of clients or third persons because the lawyer is acting or has acted as a lawyer in a client-lawyer relationship, or when the lawyer is acting as a Fiduciary, or as an escrow agent, a settlement agent or a representative payee, or as an agent, having been designated as such by a client or having been so selected as a result of a client-lawyer relationship or the lawyer's status as such. Securities should be appropriately safeguarded. All property which is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property and, if Rule 1.15 Funds, in one or more Trust Accounts, or, if a Fiduciary entrustment, in an investment or account authorized by applicable law or a governing instrument. The responsibility for identifying an account as a Trust Account shall be that of the lawyer in whose name the account is held. Whenever a lawyer holds Rule 1.15 Funds, the lawyer must maintain at least two accounts: one in which those funds are held and another in which the lawyer's own funds may be held.

(2) A lawyer should maintain on a current basis books and records in accordance with sound accounting practices consistently applied and comply with any recordkeeping rules established by law or court order, including those records identified in paragraph (c). With little exception, funds belonging to a client or third party must be deposited into a Trust Account as defined in paragraph (a)(11), and funds belonging to the lawyer must be deposited in a business operating account maintained pursuant to paragraph (j). Thus, unless the client gives informed consent, confirmed in writing, to a different manner of handling funds advanced by the client to cover fees and expenses, the lawyer must deposit those funds into a Trust Account pursuant to paragraph (i). If the lawyer pools such funds belonging to more than one client, under paragraph (c)(2) the lawyer must keep a ledger for each individual client, regularly recording all funds received from the client and their purpose, and all disbursements of earned fees and expenses incurred. As fees become earned, the lawyer must promptly transfer those funds to the operating account. If the lawyer pools client funds after settlement or verdict in a single Trust Account, the lawyer must maintain a ledger of receipts and disbursements for each individual client, regularly recording the dates of each transaction, the identity of payors and payees, and the purpose of each disbursement, withdrawal or transfer of funds. The requirement of monthly reconciliations should deter situations where an attorney's Trust Account contains a shortfall for any significant period of time. Additionally, if a lawyer fails to maintain the records identified in paragraph (c) or to perform the required monthly reconciliations, later claims by the lawyer that a shortfall (i.e., misappropriation) resulted from negligence, even if credible, will necessarily be balanced against the lawyer's abdication of responsibility to comply with essential requirements associated with acting as a fiduciary and serving in a position of trust. The failure to maintain or timely produce the records required by paragraph (c) hampers rule-mandated or agency-promulgated investigative inquiries by the Pennsylvania Lawyers Fund for Client Security and the Office of Disciplinary Counsel and may serve as a basis for emergency temporary suspension of the lawyer's license to practice law. See Pa.R.D.E. 208(f)(1), 208(f)(5), 213(g)(2) and 221(g)(3).

(3) While normally it is impermissible to commingle the lawyer's own funds with Rule 1.15 Funds, paragraph (h) provides that it is permissible when necessary to pay service charges on that account. Accurate records must be kept regarding the funds.

(4) A lawyer's obligations with respect to funds of clients and third persons depend on the capacity in which the lawyer receives them, on whether they are Fiduciary Funds as defined in paragraph (a)(3) and on whether they are Nonqualified Funds or Qualified Funds as defined in paragraphs (a)(8) or (9) respectively. If the lawyer receives them in one of the capacities identified in paragraph (a)(10), the obligations in paragraphs (b) through (h), such as safeguarding, notification, and recordkeeping, apply. Nonqualified Funds other than Fiduciary Funds are to be placed in a Non-IOLTA Account, as defined in paragraph (a)(7), in an Eligible Institution, as defined in paragraph (a)(1), unless the client or third person specifically agrees to

another investment vehicle for the benefit of the client or third person. Qualified Funds other than Fiduciary Funds must, subject to certain exceptions, be placed in an IOLTA Account defined in paragraph (a)(5).

(5) If the funds, whether Qualified Funds or Nonqualified Funds, are Fiduciary Funds, they may be placed in an investment or account authorized by the law applicable to the entrustment or authorized by the terms of the instrument governing the Fiduciary Funds. In such investment or account they shall be subject to the obligations of safeguarding, notification and recordkeeping. This Rule is not intended to change the substantive law or procedural rules that govern Fiduciary Funds or property with the exception of the specific recordkeeping requirements, segregation of Fiduciary Funds or property, and where Fiduciary Funds are kept in an Eligible Institution, overdraft reporting pursuant to Pa.R.D.E. 221, to the extent that those requirements underscore or supplement the requirements regarding Fiduciary Funds or property. The goal of the amendments is to require all attorneys to keep appropriate records of entrusted funds, segregate such funds from the attorney's funds, account to those with an interest in the funds, and distribute the funds when due, and to permit the disciplinary system to respond when lawyers fail to comply with these standards.

(6) This Rule does not require a Fiduciary to liquidate entrusted investments or investments made in accordance with applicable law or a governing instrument or to transfer non-income producing fiduciary account balances to an IOLTA Account. This Rule does not prohibit a Fiduciary from making an investment in accordance with applicable law or a governing instrument. Funds which are controlled by a non-lawyer professional co-fiduciary shall not be considered to be Rule 1.15 Funds for the purposes of this Rule.

(7) Lawyers often receive funds from which the lawyer's fee will be paid. Unless the fee is non-refundable, it should be deposited to a Trust Account and drawn down as earned. The lawyer is not required to remit to the client funds that the lawyer reasonably believes represent fees owed. However, a lawyer may not hold funds to coerce a client into accepting the lawyer's contention. The disputed portion of the funds must be kept in a Trust Account and the lawyer should suggest means for prompt resolution of the dispute, such as arbitration. The undisputed portion of the funds shall be promptly distributed.

(8) Third parties may have lawful claims against specific funds or other property in a lawyer's custody such as a client's creditor who has a lien on funds recovered in a personal injury action. A lawyer may have a duty under applicable law to protect such third-party claims against wrongful interference by the client. In such cases, when the third party claim is not frivolous under applicable law, the lawyer must refuse to surrender the property to the client unless the claims are resolved. A lawyer should not unilaterally assume to arbitrate a dispute between the client and the third party. When there are substantial grounds for dispute as to the person entitled to the funds, the lawyer may file an action to have a court resolve the dispute.

(9) Other applicable law may impose pertinent obligations upon a lawyer independent of and in addition to the obligations arising from this Rule. For example, a lawyer who receives funds as an escrow agent, a representative payee, or a Fiduciary remains subject to the law applicable to the entrustment, such as the Probate, Estates and Fiduciaries Code, Orphans' Court Rules, the Social Security Act, and to the terms of the governing instrument. If, during the final year of a Fiduciary entrustment, the lawyer who is serving as a Fiduciary reasonably expects that the funds cannot earn income for the client or third person in excess of the cost incurred to secure such income while the funds are held, the lawyer may, in the discretion of the lawyer, deposit the funds into the IOLTA Account of the lawyer, or may arrange to discontinue the payment of interest on the segregated Trust Account.

(10) A lawyer must participate in the Pennsylvania Lawyers Fund for Client Security established in Rule 503 of the Pennsylvania Rules of Disciplinary Enforcement. It is a means through the collective efforts of the bar to reimburse persons who have lost money or property as a result of dishonest conduct of a lawyer.

(11) Paragraphs (q) through (t) provide for the Interest on Lawyer Trust Account (IOLTA) program. There are further instructions relating to the IOLTA program in Rules 219 and 221 of the Pennsylvania Rules of Disciplinary Enforcement and in the Regulations of the Interest On Lawyers Trust Account Board, *204 Pa. Code, § 81.1* et seq., which are referred to as the IOLTA Regulations.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 1.18

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 1.18. Duties to Prospective Clients

(a) A person who consults with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.

(b) Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal information which may be significantly harmful to that person, except as Rule 1.9 would permit with respect to information of a former client.

(c) A lawyer subject to paragraph (b) shall not represent a client with interests materially adverse to those of a prospective client in the same or a substantially related matter if the lawyer learned information from the prospective client that could be significantly harmful to that person in the matter, except as provided in paragraph (d). If a lawyer is disqualified from representation under this paragraph, no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter, except as provided in paragraph (d).

(d) When a lawyer has learned information as defined in paragraph (c), representation is permissible if:

(1) both the affected client and the prospective client have given informed consent, or;

(2) all of the following apply:

(i) the disqualified lawyer took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client;

(ii) the disqualified lawyer is screened from any participation in the matter and is apportioned no part of the fee therefrom; and

(iii) written notice is promptly given to the prospective client.

History

SOURCE:

The provisions of this Rule 1.18 amended October 22, 2013, effective in 30 days, *43 Pa.B. 6641.* Immediately preceding text appears at serial pages (343163) to (343164) and (361483).

Annotations

Notes

NOTES:

Commentary

Comment:

(1) Prospective clients, like clients, may disclose information to a lawyer, place documents or other property in the lawyer's custody, or rely on the lawyer's advice. A lawyer's consultations with a prospective client usually are limited in time and depth and leave both the prospective client and the lawyer free (and sometimes required) to proceed no further. Hence, prospective clients should receive some but not all of the protection afforded clients.

(2) A person becomes a prospective client by consulting with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter. Whether communications, including written, oral, or electronic communications, constitute a consultation depends on the circumstances. For example, a consultation is likely to have occurred if a lawyer, either in person or through the lawyer's advertising in any medium, specifically requests or invites the submission of information about a potential representation without clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations, and a person provides information in response. See also Comment (4). In contrast, a consultation does not occur if a person provides information to a lawyer, such as in an unsolicited e-mail or other communication, in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest. Such a person communicates information unilaterally to a lawyer without any reasonable expectation that a client-lawyer relationship will be established, and is thus not a "prospective client." A person who participates in an initial consultation, or communicates information, with the intent to disqualify a lawyer from representing a client with materially adverse interests is not entitled to the protections of paragraphs (b) or (c) of this Rule. A person's intent to disqualify may be inferred from the circumstances.

(3) It is often necessary for a prospective client to reveal information to the lawyer during an initial consultation prior to the decision about formation of a client-lawyer relationship. The lawyer often must learn such information to determine whether there is a conflict of interest with an existing client and whether the matter is one that the lawyer is willing to undertake. Paragraph (b) prohibits the lawyer from using or revealing significantly harmful information, except as permitted by Rule 1.9, even if the client or lawyer decides not to proceed with the representation. The duty exists regardless of how brief the initial conference may be.

(4) In order to avoid acquiring disqualifying information from a prospective client, a lawyer considering whether or not to undertake a new matter should limit the initial consultation to only such information as reasonably appears necessary for that purpose. Where the information indicates that a conflict of interest or other reason for non-representation exists, the lawyer should so inform the prospective client or decline the representation. If the prospective client wishes to retain the lawyer, and if consent is possible under Rule 1.7, then consent from all affected present or former clients must be obtained before accepting the representation.

(5) A lawyer may condition a consultation with a prospective client on the person's informed consent that no information disclosed during the consultation will prohibit the lawyer from representing a different client in the matter. See Rule 1.0(e) for the definition of informed consent. If the agreement expressly so provides, the prospective client may also consent to the lawyer's subsequent use of information received from the prospective client.

(6) Even in the absence of an agreement, under paragraph (c) the lawyer is not prohibited from representing a client with interests adverse to those of the prospective client in the same or a substantially related matter unless the lawyer has received from the prospective client information that could be significantly harmful if used in the matter.

(7) Under paragraph (c), the prohibition in this Rule is imputed to other lawyers as provided in Rule 1.10, but, under paragraph (d)(1), imputation may be avoided if the lawyer obtains the informed consent of both the prospective and affected clients. In the alternative, imputation may be avoided if the conditions of paragraph (d)(2) are met and all disqualified lawyers are timely screened and written notice is promptly given to the prospective client. See Rule 1.0(k) (requirements for screening procedures). Paragraph (d)(2)(ii) does not prohibit the screened lawyer from receiving a salary or partnership share established by prior independent agreement, but that lawyer may not receive compensation directly related to the matter in which the lawyer is disqualified.

(8) Notice, including a description of the screened lawyer's prior representation and of the screening procedures employed, generally should be given as soon as practicable after the need for screening becomes apparent.

(9) For the duty of competence of a lawyer who gives assistance on the merits of a matter to a prospective client, see Rule 1.1. For a lawyer's duties when a prospective client entrusts valuables or papers to the lawyer's care, see Rule 1.15.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 5.1

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 5.1. Responsibilities of Partners, Managers and Supervisory Law yers

(a) 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.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Annotations

Notes

NOTES:

Commentary

Comment:

(1) Paragraph (a) applies to lawyers who have managerial authority over the professional work of a firm. See Rule 1.0(c). This includes members of a partnership, the shareholders in a law firm organized as a professional corporation, and members of other associations authorized to practice law; lawyers having comparable managerial authority in a legal services organization or a law department of an enterprise or government agency; and lawyers who have intermediate managerial responsibilities in a firm. Paragraph (b) applies to lawyers who have supervisory authority over the work of other lawyers in a firm.

(2) Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct. Such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.

(3) Other measures that may be required to fulfill the responsibility prescribed in paragraph (a) can depend on the firm's structure and the nature of its practice. In a small firm of experienced lawyers, informal supervision and periodic review of compliance with the required systems ordinarily will suffice. In a large firm, or in practice situations in which difficult ethical problems frequently arise, more elaborate measures may be necessary. Some firms, for example, have a procedure whereby

junior lawyers can make confidential referral of ethical problems directly to a designated senior partner or special committee. See Rule 5.2. Firms, whether large or small, may also rely on continuing legal education in professional ethics. In any event, the ethical atmosphere of a firm can influence the conduct of all its members and the partners may not assume that all lawyers associated with the firm will inevitably conform to the Rules.

(4) Paragraph (c) expresses a general principle of personal responsibility for acts of another. See also Rule 8.4(a).

(5) Paragraph (c)(2) defines the duty of a partner or other lawyer having comparable managerial authority in a law firm, as well as a lawyer who has direct supervisory authority over performance of specific legal work by another lawyer. Whether a lawyer has supervisory authority in particular circumstances is a question of fact. Partners and lawyers with comparable authority have at least indirect responsibility for all work being done by the firm, while a partner or manager in charge of a particular matter ordinarily also has supervisory responsibility for the work of other firm lawyers engaged in the matter. Appropriate remedial action by a partner or managing lawyer would depend on the immediacy of that lawyer's involvement and the seriousness of the misconduct. A supervisor is required to intervene to prevent avoidable consequences of misconduct if the supervisor knows that the misconduct occurred. Thus, if a supervising lawyer knows that a subordinate misrepresented a matter to an opposing party in negotiation, the supervisor as well as the subordinate has a duty to correct the resulting misapprehension.

(6) Professional misconduct by a lawyer under supervision could reveal a violation of paragraph (b) on the part of the supervisory lawyer even though it does not entail a violation of paragraph (c) because there was no direction, ratification or knowledge of the violation.

(7) Apart from this Rule and Rule 8.4(a), a lawyer does not have disciplinary liability for the conduct of a partner, associate or subordinate. Whether a lawyer may be liable civilly or criminally for another lawyer's conduct is a question of law beyond the scope of these Rules.

(8) The duties imposed by this Rule on managing and supervising lawyers do not alter the personal duty of each lawyer in a firm to abide by the Rules of Professional Conduct. See Rule 5.2(a).

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document

204 Pa. Code Part V, Subpt A, Ch 81, Subch A, Rule 5.3

This document is current through the April 2017 supplement Changes effective through 47 Pa.B. 812 (February 4, 2017)

Rule 5.3. Responsibilities Regarding Nonlawyer Assistance

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner 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 the person's conduct is compatible with the professional obligations of the lawyer.

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

History

SOURCE:

The provisions of this Rule 5.3 amended October 22, 2013, effective in 30 days, *43 Pa.B. 6641.* Immediately preceding text appears at serial pages (309457) to (309458).

Annotations

Notes

NOTES:

Commentary

Comment:

(1) Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that nonlawyers in the firm and nonlawyers outside the firm who work on firm matters act in a way compatible with the professional obligations of the lawyer. See Comment (6) to Rule 1.1 and Comment (1) to Rule 5.1. Paragraph (b) applies to lawyers who have supervisory authority over such nonlawyers within or outside the firm. Paragraph (c) specifies the circumstances in which a lawyer is responsible for conduct of a nonlawyer that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer.

Nonlawyers Within the Firm

(2) Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.

Nonlawyers Outside the Firm

(3) A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including 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. See also Rules 1.1, 1.2, 1.4, 1.6, 5.4(a), and 5.5(a). When retaining or directing a nonlawyer outside the firm, a lawyer 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.

(4) Where the 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. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Research References & Practice Aids

HIERARCHY NOTES:

Title Note

Subchapter Note

End of Document