[DRAFT]

[THIS CLAWBACK STIPULATION IS INTENDED FOR USE IN FEDERAL COURT AND INCLUDES REFERENCE TO FRCP 26(b)(5)(B) AND FRE 502 (d) WHICH GOVERN INADVERTENT PRODUCTION OF DOCUMENTS. HOWEVER, THE CLAWBACK ELIMINATES AND OBVIATES THE NEED FOR A PARTY TO PROVE IT TOOK REASONABLE STEPS TO PREVENT PRIVILEGE AS REQUIRED IN FRCP 26(b)(5). BE SURE TO CAREFULLY CONSIDER THE DEADLINES IMPOSED BY THIS AGREEMENT (I.E., TIME TO RESPOND TO RETURN DEMAND) AND MAKE SURE THEY ARE REASONABLE FOR YOUR CASE. ALSO NOTE THAT THIS CLAWBACK HAS A COST-SHIFTING PROVISION IN THE EVENT THAT THE PRODUCING PARTY INSISTS ON THE RETURN OF ELECTRONIC COPIES RATHER THAN THEIR SEQUESTER OR DISABLEMENT. IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT THE FIRM'S EDISCOVERY COUNSEL]

IN THE UNITED STATES DISTRICT COURT
FOR THE ________ DISTRICT OF _______

[PLAINTIFFS],	
Plaintiffs,	**CIV. NO.:**
v.	
[DEFENDANTS],	
Defendants.	

CLAWBACK AND PRESUMPTIVELY PRIVILEGED PROTOCOL STIPULATION AND FRE 502(D) AND (E) ORDER

The parties hereby stipulate to protect certain privileged and otherwise protected documents and electronically stored information (collectively, "document" or "documents") against claims of waiver in the event they are produced during the course of this litigation whether pursuant to a Court Order, a parties' discovery request or informal production.

Both parties may be required to produce large volumes of documents and, to comply with discovery deadlines in the case, wish to complete discovery as expeditiously as possible, while preserving and without waiving any evidentiary protections or privileges applicable to the information contained in the documents produced, including as against third parties and other Federal and State proceedings. Accordingly, the parties hereby stipulate to, and the Court hereby Orders pursuant to Federal Rules of Civil Procedure 502(d) and (e), as follows:

1. The inadvertent production of any document in this action shall be without prejudice to any claim that such material is protected by any legally cognizable privilege or evidentiary protection including, but not limited to the attorney-client privilege, or the work product doctrine, and no party shall be held to have waived any rights by such inadvertent production.

2. If any document produced by another party is on its face subject to a legally recognizable privilege or evidentiary protection, the receiving party shall: (a) refrain from reading the document any more closely than is necessary to ascertain that it is privileged; (b) immediately notify the producing party in writing that it has discovered documents believed to be privileged or protected; (c) specifically identify the documents by Bates number range or hash value range, and, (d) where possible, return, sequester, or destroy all copies of such documents, along with any notes, abstracts or compilations of the content thereof, within five (5) days of discovery by the receiving party. Where such documents cannot be destroyed or separated it shall not be reviewed, disclosed, or otherwise used by the receiving party. Notwithstanding, the receiving party is under no obligation to search or review the producing party's documents to identify potentially privileged or work product protected documents.

3. Upon written notice of an unintentional production by the producing party or oral notice if notice is delivered on the record at a deposition, the receiving party must promptly return, sequester or destroy the specified document and any hard copies the receiving party has and may not use or disclose the information until the privilege claim has been resolved. The producing party shall also provide an updated privilege log for such documents setting forth the author, recipient(s), subject matter of the document, along with the basis for the claim of privilege or evidentiary protection, as well as any portion of the document that does not contain privileged or protected information. To the extent that the producing party insists on the return or destruction of electronic copies, rather than disabling the documents from further use or otherwise rendering them inaccessible to the receiving party, the producing party shall bear the costs of the return or destruction of such electronic copies.

4. To the extent that the information contained in a document subject to a claim has already been used in or described in other documents generated or maintained by the receiving party, then the receiving party will sequester such documents until the claim has been resolved. If the receiving party disclosed the specified documents before being notified of its inadvertent production, it must take reasonable steps to retrieve it. The producing party shall preserve the specified documents until the claim is resolved.

5. The receiving party shall have five (5) days from receipt of notification of the inadvertent production to determine in good faith whether to contest such claim and to notify the producing party in writing of an objection to the claim of privilege and the grounds for that objection.

6. The receiving party's return, sequestering or destruction of such privileged or protected documents as provided herein will not act as a waiver of the requesting party's right to move for the production of the returned, sequestered or

destroyed documents on the grounds that the documents are not in fact subject to a viable claim of privilege or protection. However, the receiving party is prohibited and estopped from arguing that the production of the documents in this matter acts as a waiver of an applicable privilege or evidentiary protection, that the disclosure of the documents was not inadvertent, that the producing party did not take reasonable steps to prevent the disclosure of the privileged documents or that the producing party failed to take reasonable steps to rectify the error as set forth in Federal Rules of Civil Procedure 26(b)(5)(B). The producing party need make no showing with respect to measures take to prevent the inadvertent production of the documents in question in order to be entitled to their return.

7. Either party may submit the specified documents to the Court under seal for a determination of the claim and will provide the Court with the grounds for the asserted privilege or protection. The receiving party may not use the documents for any purpose absent this Court's Order. Any party may request expedited treatment of any request for the Court's determination of the claim.

8. Upon a determination by the Court that the specified documents are protected by the applicable privilege or evidentiary protection, and if the specified documents have been sequestered rather than returned or destroyed, the specified documents shall be returned or destroyed. The Court may also order, the identification and/or review of documents that have been identified as being potentially subject to a legally recognized claim by search terms or other means.

9. [Upon a determination by the Court that the specified documents are not protected by the applicable privilege, the producing party shall bear the costs of placing or restoring the information into any programs or databases from which it was removed or destroyed and render accessible any documents that were disabled or rendered inaccessible, unless otherwise ordered by the Court.]

So Stipulated:

Plaintiff’s Law Firm	Defendant’s Law Firm
By: ________________________	By:________________________

[DONE AND ORDERED]:
[SO ORDERED]:

____

Glossary

Most entries in this glossary were derived, with permission, from *The Sedona Conference Glossary: E-Discovery & Digital Information Management* (3d ed. 2010), *available at* https://thesedonaconference.org/download-pub/471.

active data (active records): Information located in a computer system's memory or in storage media attached to the system (e.g., disk drives) that is readily available to the user, to the operating system, and to application software. (See *storage medium.*)

application: One or more related software programs that enable a user to enter, store, view, modify, or extract information from files or databases. The term is commonly used in place of *program* or *software.* Applications may include word processors, Internet browsing tools, spreadsheets, e-mail clients, personal information managers (contact information and calendars), and other databases.

archival data: Information that is maintained in long-term storage for business, legal, regulatory, or similar purposes, but not immediately accessible to a computer system's user. The data may be stored on removable media, such as CDs, tapes, or removable disk drives, or may be maintained on system disk drives. The data are typically stored in an organized way to help identify, access, or retrieve individual records or files.

attachment: A record or file associated with another record for the purpose of retention, transfer, processing, review, production, or routine records management. There may be multiple attachments associated with a single "parent" or "master" record. In many records and information management programs, or in a litigation context, the attachments and associated records may be managed and processed as a single unit. In common use, this term often refers to a file (or files) associated with an e-mail message for retention and storage as a single message unit.

backup data (disaster recovery data): An exact copy of data that serves as a source for recovery in the event of a system problem or disaster. The data are generally stored separately from active data on tapes or removable disk drives, and often without indexes or other information. As a result, the data are in a form that makes it difficult to identify, access, or retrieve individual records or files.

backup tape recycling: A process in which backup data tapes are overwritten with new backup data, usually according to a fixed schedule determined jointly by records-management, legal, and information technology (IT) personnel.

cloud computing: "[A] model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." http://csrc.nist.gov/groups/SNS/cloud-computing/ (last visited June 22, 2010). For further explanation, see the NIST website cited.

computer forensics: The scientific examination and analysis of computerized data primarily for use as evidence. Computer forensics may include the secure collection of computer data; the examination of suspect data to determine details, such as origin and content; and the presentation of computer-based information to courts. It may involve re-creating deleted, damaged, or missing files from disk drives; validating dates and authors or editors of documents; and certifying key elements of electronically stored information.

data (electronic): Information stored on a computer, including numbers, text, and images. Computer programs (e.g., word processing software, spreadsheet software, presentation software) are used to process, edit, or present data.

data mining: Generally refers to knowledge discovery in databases (structured data). It relies on automatic and semiautomatic techniques to extract previously unknown interesting patterns from large quantities of data, which can then be subjected to further inspection and analysis. In the context of electronic discovery, this term often refers to the processes used to sort through a collection of electronically stored information to extract evidence for production or presentation in an investigation or in litigation.

de-duplication: A process that searches for and deletes duplicate information. (See the glossary maintained by The Sedona Conference for a description of different types of de-duplication.)

deleted data: Data that once existed on a computer as active data, but have been marked as deleted by computer programs or user activity. Deleted data may remain on the storage media in whole or in part until they are overwritten or "wiped." Even after the data have been wiped, directory entries, pointers, or other information relating to the deleted data may remain on the computer.

deletion: A process in which data are marked as deleted by computer programs or user activity and made inaccessible except through the use of special data-recovery tools. Deletion makes data inaccessible with normal application programs, but commonly leaves the data on the storage medium. There are different degrees of deletion. "Soft-deleted data" are data marked as deleted in the computer operating system (and not generally available to the user after such marking), but not yet physically removed from or overwritten on the storage medium. Soft-deleted data can often be restored in their entirety. In contrast, "wiping" is a process that overwrites the deleted data with random digital characters, rendering the data extremely difficult to recover, and "degaussing" is a process that rearranges the magnetic patterns on the medium, rendering the data impossible to recover with all but the most sophisticated computer forensics tools.

disk mirroring: The ongoing process of making an exact copy of information from one location to another in real time. It is often used to protect data from a catastrophic hard disk failure or for long-term data storage. (See *replication.*)

electronic discovery: The process of collecting, preparing, reviewing, and producing electronic documents in a variety of criminal and civil actions and proceedings.

embedded data: Data that include commands that control or manipulate data, such as computational formulas in spreadsheets or formatting commands in a word processing document. Embedded data are not visible when a document is printed or saved as an image format. (See *metadata.*)

ESI: Electronically stored information.

file format: The internal organization, characteristics, and structure of a file that determine the software programs with which it can optimally be used, viewed, or manipulated. The simplest file format is ASCII (American Standard Code for Information Interchange; pronounced "ASK-ee"), a nonproprietary text format. Documents in ASCII consist of only text with no formatting or graphics and can be read by most computer systems using nonproprietary applications. Specific applications may define unique (and proprietary) formats for their data (e.g., WordPerfect document file format). These formats are also called the "native" format. Files with unique formats may only be viewed or printed with their originating application or an application designed to work with compatible formats. Computer systems commonly identify files by a naming convention that denotes the native format (and therefore the probable originating application) as an extension of the file's name. For example, a WordPerfect document could be named document.wpd, where ".wpd" denotes a WordPerfect file format. Other common formats are .docx for Microsoft Word files, .xls for Microsoft Excel spreadsheet files, .txt for ASCII text files, .ppt for Microsoft PowerPoint files, .jpg for photographs or other images, and .pdf for Adobe Acrobat documents.

forensic copy: An exact copy of an entire physical storage medium (e.g., hard drive, CD, DVD, tape), including all active and residual data and unallocated, or slack, space on the medium. Forensic copies are often called "images" or "imaged copies."

form of production: The manner in which requested documents are produced. The term is used to refer to both the file format and the media on which the documents are produced (paper versus electronic).

hash value: A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical identifiers so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

image (verb): To image a hard drive is to make an identical copy of the hard drive at the lowest level of data storage. The image will include deleted data, residual data, and data found in hidden portions of the hard drive. Imaging is also known as creating a "bit stream image" or "mirror image," or "mirroring" the drive. It is different from the process of making a "logical copy" of or "ghosting" a hard drive, which normally copies only the active data on the hard drive, and not the deleted data, residual data, and data in hidden portions of the hard drive.

legacy data: Electronically stored information in which an organization may have invested significant resources and which retains importance, but which was created and is stored through the use of software and/or hardware that has become obsolete or replaced ("legacy systems"). Legacy data may be costly to restore or reconstruct.

metadata: Information about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified; its size; and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden from users but are still available to the operating system or the program used to process the data set or document. (See *embedded data* and *systems data.*)

near-line data storage: Storage in a system that is not physically part of the computer system or local network in daily use, but can be accessed through the network. Near-line data may be stored in a library of CDs, which can be automatically located and loaded for reading, or stored at a remote location accessible through an Internet connection. There is usually a small time lag between the request for data stored in near-line media and the data's availability to an application or user. Making near-line data available is an automated process (in contrast, making "offline" data available generally can be done only by a person physically retrieving the data).

offline data storage: The storage of electronic records, often for long-term archival purposes, on removable media (e.g., CDs, removable disk drives) or magnetic tape that is not connected to a computer or network. Accessing offline media usually requires manual intervention and is much slower than accessing online or near-line media.

PDF (portable document format): A file format developed by Adobe Systems Incorporated. Once converted to this format, documents are readable outside of the application that created them. A PDF file captures document formatting information (e.g., margins, spacing, fonts) from the original application (e.g., WordPerfect) in such a way that the document can be viewed and printed as intended in the original application by the Adobe Reader program, which is available for most computer operating systems. Other programs (most notably Adobe Acrobat) are required to edit or otherwise manipulate a PDF file.

records management: The activities involved in handling information, generally for organizations that are large data producers. Records management includes maintaining, organizing, preserving, and destroying information, regardless of its form or the medium on which it is stored.

replication: The ongoing process of making an exact copy of information from one location to another in real time. It is often used to protect data from a catastrophic failure or for long-term data storage. (See *disk mirroring.*)

residual data (ambient data): Data that are not active on a computer system and that are not visible without the use of "undelete" or other special data-recovery techniques. Residual data may contain copies of deleted files, Internet files, and file fragments.

restore: To transfer data from a backup or archival storage system (e.g., tapes) to an online system. Restoring archival data may require replication of the original hardware and software operating environment.

sampling: The process of selecting a small part of a larger data source and searching it to test for the existence, or frequency, of relevant information, to assess whether the source contains privileged or protected information, and to assess the costs and burdens of identifying and producing requested information.

search engine: A program that enables a search for key words or phrases, such as on web pages throughout the World Wide Web. (See the glossary maintained by The Sedona Conference for a description of different types of searches.)

storage medium: The physical device containing electronically stored information, including computer memory, disk drives (including removable disk drives), magneto-optical media, CDs, DVDs, memory sticks, and tapes.

systems data: Information about a computer system that includes when people logged on and off a computer or network, the applications and passwords they used, and what websites they visited.

PRIVILEGED ATTORNEY CLIENT COMMUNICATION/ATTORNEY WORK PRODUCT

PLEASE DO NOT FORWARD WITHOUT PRIOR CONSENT OF LEGAL DEPT.

To:	Distribution (See Attached)
From:	[In-house lawyer]
Subject:	**DOCUMENT HOLD AND PRESERVATION NOTIFICATION**
Date:	[________]

[Company name] ("Company") has received notice of a [potential/pending] claim relating to [describe subject matter of claim], as to which legal counsel advises that the Company should take steps to preserve and maintain documents and data relating [subject matter]. The Company requires your compliance to meet these preservation obligations. In order to ensure our effective cooperation and to avoid any possibility that the Company faces adverse consequences for failure to properly preserve relevant information, it is essential that all potentially relevant documents be preserved.

To comply with its obligations, the Company is preserving records, documents, data, and all forms of electronically stored information (collectively "Documents") related to the [subject matter] described above. [May include list of the subjects/topics, and typical types of Documents, likely to be potential relevant.]

The Company may be required to produce these Documents at some point in the future. Therefore, Documents that relate to [subject matter] are subject to the requirements set forth in this Notification. We recognize that this description is very broad in scope; however, at the present time, we do not have additional information to permit us to limit the scope of any potential document collection. Your immediate action in retaining and preserving these Documents is needed to protect the Company's interests.

It is vital that you do not destroy, discard or delete any Documents, whether paper or electronic (including e-mail), having anything to do with the [subject matter]. Please take all steps necessary to suspend routine document destruction activities that might threaten such Documents regardless of their location (*e.g.*, in your office, at your home, in off-site storage), and regardless of what form in which they are stored (*e.g.*, in hard copy files, in your Company e-mail account, on the hard drive of your office or home computer, on electronic media such as CD/DVDs and thumb drives, in your personal e-mail account, your Blackberry or other PDA). This includes turning off any "auto-delete" functions on any device that you control. In addition, it is very important that you preserve and do not destroy all passwords, decryption procedures, including software, to decrypt the files, network access codes, I.D. names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view, and if necessary, reconstruct the electronically stored information relating to the issues discussed herein. If you have any doubt as to whether something should be saved, you should err on the side of preservation.

Electronically stored information includes, by way of example and not as an exclusive list, potentially relevant information electronically, magnetically, optically, or otherwise stored as:

(1) digital communications, e.g., e-mail, voice mail, instant messaging (to the extent possible);
(2) e-mail server stores, e.g., Lotus Domino, NSF, Microsoft Exchange, BDB;
(3) word processed documents, e.g., Word or WordPerfect files and drafts;
(4) spreadsheets and tables;
(5) accounting application data;
(6) image and facsimile files;
(7) sound recordings;
(8) video and animation;
(9) databases, e.g., Access, Oracle, SQL Server data, SAP;
(10) contact and relationship management data, e.g., Outlook ACTI;
(11) online access data, e.g., temporary internet files, history, cookies;
(12) presentations;
(13) network access and server activity logs;
(14) project management application data;
(15) computer aided design/drawing files;
(16) backup and archival files stored on any media, including but not limited to, hard drives, file servers, storage area network, remote backup service, solid-state drives, flash memory, thumb drives, floppy disks, compact discs, DVD's, magnetic tapes or zip disks; and
(17) calendar data (e.g. Outlook PST).

You have received this memorandum because you have been identified as someone in the Company who may either personally possess Documents pertaining to the [subject matter], or manage an organization in which such information resides. If you possess any such Documents, please notify [contact in legal department] at [telephone number] or [email address] so that arrangements can be made to review the Documents and take appropriate steps to secure them in accordance with legal requirements. If you believe this Notification should be directed to someone who may have relevant Documents but was not identified on the attached Distribution List, whether within your organization or otherwise, including outside consultants, advisors and contractors, please advise [contact in legal department] so that appropriate measures can be taken. In the event you do not possess any Documents described in this Notification, please notify [contact in legal department] so that we can ensure all avenues of preservation have been exhausted.

Your compliance with the instructions in this hold memorandum is critically important. Any concealment, alteration or destruction of responsive Documents may in itself constitute a violation of law and could result in significant adverse consequences for the Company.

Thank you for your immediate attention to this matter. Please do not hesitate to contact [contact in legal department] at [phone number/email address] if you have any questions or concerns.

STEVEN WILLIAM TEPPLER
CURRICULUM VITAE

Current:

Partner
Kirk•Pinkerton, PA
240 So. Pineapple Avenue, 6th Floor
Sarasota, FL 34236
Chicago, IL, 60654
Telephone: 941.364.2410
G-Voice: 941.487.0050
Facsimile: 941.364.2490
Email: steppler@kirkpinkerton.com

Electronic Discovery and Information Governance Practice:

Chairs Kirk-Pinkerton's electronic discovery (pre-discovery through trial) and information governance practice, and leads the Kirk-Pinkerton consulting group. Practice focus is upon electronic discovery, digital evidence life-cycle management, preservation, loss or destruction of electronically stored information, authentication and admissibility issues uniquely inherent to computer-generated information, including asserting and defending discovery abuse and spoliation issues arising from inadvertent, unauthorized or illegal data manipulation or alteration. Leads the firm's HIPAA risk profiling, liability exposure and breach response/remediation and notification practice. Consults, litigates, and advises to the private and public sectors about risk and liability unique to information governance and digital evidence life cycle management, including compliance issues arising under Sarbanes-Oxley Act; Dodd-Frank Act; Gramm Leach Bliley Act, HIPAA, and 21 CFR Part 11. Founding principal of TimeCertain, LLC a provider of enterprise level content authentication technology and digital data content life-cycle consulting services to both the public and private sectors. Inventor, with six patents issued for content authentication technology. Founding co-chair of the Electronic Discovery and Digital Evidence Practitioner's Workshop (an American Bar Association National Institute). Member of Florida Bar Business Law Section eDiscovery Committee, co-drafter of electronic discovery amendments to the Florida Rules of Civil Procedure.

Admitted to Practice:

New York

Supreme Court of New York: January 1981
United States District Court for the Southern District of New York: September 1981
United States District Court for the Eastern District of New York: September 1981
United States District Court for the Western District of New York: July 2011
United States Court of Appeals for the Second Circuit: October 2009

District of Columbia

District of Columbia Court of Appeals: June 1995
United States District Court for the District of Columbia: September 1995
United States Court of Appeals for the District of Columbia Circuit: October 2000
United States Court of Appeals for the Federal Circuit; February 1996

Florida
Supreme Court of the State of Florida: September 2005
United States District Court for the Middle District of Florida: January 2006
United States District Court for the Southern District of Florida: July 2008
United States District Court for the Northern District of Florida: March 2012
United States Court of Appeals for the Eleventh Circuit: August 2011
Illinois
State of Illinois Supreme Court: April 2010
United States District Court for the Northern District of Illinois: May 2010

Legal and Consulting Practice:

Partner:	Kirk•Pinkerton (August 2012-Present
Partner:	Edelson McGuire, LLC (August 2009-August 2012)
Senior Counsel:	KamberEdelson, LLC (NYC) (January 2008 – July 2009)
Private Practice:	Litigation and Information Security (1995-2008)
	General Litigation (1989-1990)
Associate:	Tannenbaum, Dubin & Robinson, New York City (1980-1981)

Investment Banking Experience:
Second Vice President, Fixed Income Securities, Smith Barney Harris Upham & Co., New York, NY (1988-1989)
Senior Trader, Mortgage Backed Securities, Federal National Mortgage Association [Fannie Mae], Washington, DC (1988)
Fixed Income Securities Trader, Mabon, Nugent & Co., New York, NY (1981-1987)

Related Publications:
Testable Reliability: A Modernized Approach to Digital Evidence Admissibility (Ave Maria L. Rev. exp. Winter 2013)
Digital Evidence Life-Cycle Management: An Information Governance Approach to Defensible Generation, Preservation and Acquisition of Electronically Stored Information (editor and co-author) American Bar Association (exp. pub. Fall, 2013)
Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists, (co-author) American Bar Association, (February 2011)
Foundations of Digital Evidence, (co-author) American Bar Association (July 2008)
Life After Sarbanes-Oxley, The Merger of Information
Security and Accountability, (co-author) 45 *Jurimetrics J.* 379 (2005), American Bar Association/Arizona State University College of Law (September 2005)
ANSI Trusted Timestamping Standard, (co-author) (July 2005)
PKI Assessment Guidelines, (contributor) American Bar Association (2001)
Information Security and the Law, (contributor) Information Security Legal Manual, American Bar Association (March 2004)

Periodicals:
Electronic Discovery and Digital Evidence Digest (2009-Present)
Intersection of Law and Information Security, ISSA Magazine (January 2011)
Heightened Requirements for Encryption in U.S. Law (White Paper, December 2010)

The Pension Committee Decision, EDDE Journal (ABA Spring 2010)
Digital Evidence as Hearsay, 6 Electronic Signature Review 7 (2009)
Electronic Evidence and the CSO, CSO Magazine (October 2008)
Spoliation in the Digital Universe, The SciTech Lawyer, American Bar Association Section of Science and Technology Law (Fall 2007)
Digital Signatures Are Not Enough, (Co-Author); Information Systems Security Association (January 2006)
The Digital Signature Paradox, (Co-Author); IETF Information Workshop (The West Point Workshop June 2005)
Observations on Electronic Service of Process in the South Carolina Court System, efiling Report (June 2005)
State of Connecticut v. Swinton: A Discussion of the Basics of Digital Evidence Admissibility, (Co-Author); Georgia Bar Newsletter Technology Law Section, (Spring 2005)
The e-Filing Challenge: Generating Challenge-Proof Content and Auditable Data Part Two, eFiling Report (September 2003)
The e-Filing Challenge: Generating Challenge-Proof Content and Auditable Data Part One, eFiling Report (June 2003)
Digital Data and the Meaning of Audit, NYSSCPA Journal, (August 2002)

Security Industry Presentations:
Mock ESI Discovery Abuse/Spoliation Hearings, RSA Security Conference Law and Information Governance Track (2005-present)
Electronic Discovery Cooperation Workshop, RSA Security Conference law and Information Governance Track (April 2009)
The Technology Time Bomb – An Attorney's Ethical Obligation to Maintain Competency in Technology, Masters Seminar in Ethics, Florida Bar Annual Conference, (June 2007)
Metadata – An Ethical Minefield for Attorneys, Law and Policy Track, RSA Security Conference, San Francisco, California, (April 2007)
The Failure of the Hash Algorithm – The Sky Isn't Falling, Law and Policy Track, RSA Security Conference, San Jose, California, (February 2006)
Forensics and Digital Evidence Law, Law and Policy Track, RSA Security Conference, San Francisco, California (January 2005)
Digital Data and the Meaning of Audit, InfoSec Asia 2004 Singapore (April, 2004)
Timestamping and Audit Issues, RSA Security Conference, Law and Policy Track, San Francisco, California (February 2004)
Digital Data and the Meaning of Audit, Federal PKI Bridge Project Conference, Crystal City, Virginia (March 2003)
New Theories of Liability in an Electronic World, Internet Security Conference, Regent University, Norfolk, Virginia (January 2003)
Legal Requirements of Digital Signatures, PKI Forum Conference, Dallas, Texas (November 2002)
Achieving Digital Data Integrity, World Racing Symposium 2002, Tucson, Arizona (November 2002)

Memberships:

- Professional Ethics Committee Florida Bar (Chair, 2010-2011 Term)
- Co-Chair, American Bar Association eDiscovery and Digital Evidence Committee (2008-present)
- Co-Vice-Chair, American Bar Association Information Security Committee, Section of Science and Technology Law (2007-2010)
- American National Standards Institute, X9F4 1.31 Working Group –Trusted Transactions (2006-present)
- The Sedona Group, WG1 (2009-present)
- Editorial Board Member, ABA SciTech Lawyer (2009-present)
- Editorial Advisory Board Member, ISSA Journal (2008-present)
- American National Standards Institute, X9F4 9.95 Working Group Timestamping Protocol (2002-2005)

Education:

Juris Doctor, Benjamin N. Cardozo School of Law, New York City (1980)
Bachelor of Arts in Political Science, *Summa Cum Laude,* City College of New York, New York City (1977)