METADATA, THE CLOUD & IDENTITY THEFT

CHRIS MEUSE
KoonsFuller, P.C.
5700 W. Plano Pkwy, Suite 2200
Plano, Texas 75093
(972) 769-2727
cmeuse@koonsfuller.com

CHRIS MEUSE
KoonsFuller, P.C.
(972) 769-2727 ▪ cmeuse@koonsfuller.com
5700 W. Plano Pkwy., Suite 2200, Plano, TX 75093

EDUCATION

University of Oklahoma College of Law J.D., 2010.
University of Oklahoma, B.A. Political Science; Minor in Spanish, 2007.

CERTIFICATIONS

Board Certified in Family Law by Texas Board of Legal Specialization, 2016.

MEMBERSHIPS

- Texas Academy of Family Law Specialists
- Annette Stewart Inn of Court
- Dallas Bar Association, Family Law Section
- Collaborative Law Institute of Texas
- Bar associations: Texas, Collin County, Dallas County
- Collin County Young Lawyers Association, Director
- LeadershipSBOT

PUBLICATIONS

- *Adultery and Its Impact on Divorce*, Dallas Bar Association Headnotes, September 2011.
- *Family Law for the Non-Family Specialist: How to Master Ten Conversations on Family Law*, State Bar of Texas Litigation Update Institute, January 2012.
- *How to Answer Ten Family Law Questions*, Dallas Bar Association Headnotes, April 2013.
- *Contractual Alimony Payments to Third Parties*, Docket Call Volume 15 Issue 2, September/October 2013.
- *Digital and Virtual Assets in Divorce*, Dallas Bar Association Headnotes, February, 2014.
- *60 Websites in 60 Minutes*, 37th Annual Marriage Dissolution Institute, April 2014.
- *Digging up Digital Dirt in Family Law*, Texas Lawyer, April 2014.
- *Beam Me Up, Lawyer: Current & Trending Technology in the Family Law Practice – What Your Practice Will Need to Look Like to Survive in the Next Millennium*, FAMILY LAW TECHNOLOGY 360, December 2014.
- *Using Technology in Your Law Practice - The Basics*, 38th ANNUAL MARRIAGE DISSOLUTION INSTITUTE, April 10, 2015.
- *Utilizing Tools for Smart Presentations*, Advanced Family Law, August 6, 2015.
- *Crucial Technologies for Your Law Office*, Advanced Family Law, August 6, 2015.
- *What the Future of Your Practice May Look Like*, Annual Litigation Update, January 21, 2016.
- *Technology Competence and Update for Paralegals and Attorneys*, 34th Annual Texas Forum Agenda Towards a More Perfect Union: Attorney and Paralegal Team, March 30, 2016.
- *Managing Your Communication and Documents*, Practical Skills for New Lawyers, March 28, 2017.
- *Creative Possession Schedules*, State Bar of Texas Annual Meeting, June, 2017.
- *Bitcoin, Blockchain and Cryptocurrency*: *How it Works*, Advanced Family Law, August 2018.

AWARDS

- State Bar of Texas Star of Achievement Award for Best Series of Substantive Legal Articles, 2013.
- Super Lawyers Rising Star, 2016-17.

TABLE OF CONTENTS

I. INTRODUCTION

Metadata. The Cloud. Identity Theft. These terms are a part of our modern life and lexicon, but what are they and how do they impact our practices and clients? This paper intends to define these terms and highlight their import in today's practice.

II. METADATA

a. Metadata: Data About Data

Metadata is frequently described as "data about data." Metadata is "information describing the history, tracking, or management of an electronic file."[1] Metadata encompasses the structural information of a file that contains data about it as opposed to describing its actual substantive content. Often hidden and embedded within the original file, metadata does not normally appear on a printed page.[2]

Metadata can be found in a file's "native format." A native format retains the file structure associated with and defined by the original creating application. For example, the native format is XLS for Microsoft Excel spreadsheets and DOC for older versions of Microsoft Word documents.[3]

"Static format," as opposed to native, removes metadata from the native files. PDF, TIFF, and JPEG files are common examples of static electronic formats. Static files are created by converting native formats into static images. Static form may be searchable—to a more limited extent than native form—using optical character recognition (OCR).

Metadata can be broken down into three main categories: substantive, system and embedded.

Substantive metadata includes modifications to a document, such as prior edits or editorial comments, and codes.

System metadata includes data concerning the author, date and time of creation, and the date a document was modified. System metadata can also include information such as points of contact, an abstract of a work, keywords used in a work, a geographic location, or even an explanation of methodology.

Embedded metadata consists of text, numbers, content, data, or other information that is directly or indirectly inputted into a native file by a user and which is not typically visible to the user viewing the output display of a native file, including spreadsheet formulas, hidden columns, externally or internally linked files, such as sound files, hyperlinks, references and fields, and database information.[4]

b. Everyday Metadata

Metadata can be found in many forms: recorded voice conversations, electronic documents, text messaging or social media. Digital banking or merchant transactions involve the transfer of data, including metadata. Web content and streamed entertainment are examples of publications of data. All of us and our clients are constantly forming digital footprints, when engaging with or creating electronic information or material. Often, that digital footprint is or contains metadata.

For example, computer applications, mobile devices, and computer systems connected to the Internet collect metadata that can account for your daily Internet activities. You can see the web pages you have visited if you look at your web browsing history. You can download a history of your Facebook activities. You can obtain histories of your text messages or your telephone calls. You can access the date, time, location and address where you last attempted to fetch your Gmail email. This is only a fraction of the metadata that is created and collected from our typical, daily interactions with the digital world.

Web servers, firewalls, mobile or data network switches, and many mobile apps collect metadata. Cookies, event logging, and traffic collection are routinely collected by built in monitoring or surveillance systems. Monitoring

[1] Fed. R. Civ. P. 26(f).

[2] *In re State Farm Lloyds*, 520 S.W.3d 595, 601 (Tex. 2017).

[3] *Id*.

[4] *Aguilar v. Immigration & Customs Enf't Div. of U.S. Dep't of Homeland Sec*., 255 F.R.D. 350, 354-55 (S.D.N.Y. 2008).

or information gathering systems collect metadata for a variety of purposes from optimizing network performance or troubleshooting service problems to conducting surveillance to combat terrorism or gathering intelligence to investigate cybercrimes.

For the most part, metadata is created is harmless or even helpful. As stated above, metadata can help you find a webpage you needed or streamline your digital experiences. Because it is prevalent in our daily lives, it can also be helpful in our casework as a discovery or authentication tool, as discussed further below. But even though metadata has been described as the "new black" of electronically stored information, metadata can also get practitioners in trouble.

c. <u>Metadata: Ethics</u>

The biggest caution for lawyers regarding metadata is how metadata can inadvertently transmit confidential information. This typically occurs when tracked changes to a working document are not removed before sending a native format document to opposing counsel.

Lawyers frequently prepare and circulate electronic drafts of pleadings, orders, and agreements between clients and opposing counsel. Clients and lawyers may insert suggested revisions and comments, including those related to offers made or strengths and weakness of claims and positions. If a draft is electronically transmitted to opposing counsel without removing that metadata, it may be possible for opposing counsel to discover the comments and revisions.

To avoid this inadvertent transmission, lawyers should "scrub" electronic documents of metadata by using the word processor's built-in removal feature or separate "scrubbing" program. Further, the "Fast Saves" feature in word processors should be turned off to reduce or eliminate the accidental creation of metadata, which may be created if the document is saved while making changes or comments, along with the metadata, unbeknownst to the drafter. It is also advisable to convert a document to PDF, if possible, before sending it, reducing the chance of inadvertent transmittal of metadata.

Recently, the Professional Ethics Committee for the State Bar of Texas issued an opinion (Opinion No. 665, December 2016, 80 Tex. B.J. 46 (2017)), addressing lawyers' obligations to avoid such transmission, specifically finding that:

1. *Transmitting Lawyer:* The Texas Disciplinary Rules of Professional Conduct require lawyers to take reasonable measures to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons other than the lawyer's client. Whether a lawyer has taken reasonable measures to avoid the disclosure of confidential information in metadata will depend on the factual circumstances.

2. *Receiving Lawyer:* A Texas lawyer is required by the Texas Disciplinary Rules to avoid misleading or fraudulent use of information the lawyer may obtain from the metadata.

In coming to these conclusions, the Ethics Committee found that a lawyer's duty of competence requires lawyers who use electronic documents to understand that:

- metadata is created in the generation of electronic documents;
- transmission of electronic documents will include transmission of metadata;
- the transmitted metadata may include confidential information;
- recipients of the documents can access metadata; and
- actions can be taken to prevent or minimize the transmission of metadata.

Lawyers therefore have a duty to take reasonable measures to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons to whom such confidential information is not to be revealed pursuant to the provisions. Commonly employed methods for avoiding the disclosure of confidential information in metadata include the use of software to remove or “scrub” metadata from the document before transmission, the conversion of the document into another format that does not preserve the original metadata, and transmission of the document by fax or hard copy.

Whether a lawyer has taken reasonable measures to avoid the disclosure of confidential information in metadata will depend on the factual circumstances. Relevant factors in determining reasonableness include the steps taken by the lawyer to prevent the disclosure of the confidential information in metadata, the sensitivity of the metadata revealed, the identity of the intended recipient, and other considerations appropriate to the facts. Not every inadvertent disclosure of confidential information in metadata will violate the Disciplinary Rule.

The second issued addressed in Opinion 665 was whether the Texas Disciplinary Rules imposes particular duties on a lawyer who receives an electronic document containing metadata that appears to include confidential information of another party. The provisions of the Texas Disciplinary Rules that must be considered by lawyers with respect to the receipt of documents containing metadata are Rule 8.04(a)(3), which requires that a lawyer shall not “engage in conduct involving dishonesty, fraud, deceit or misrepresentation,” and Rule 3.03(a)(1), which requires that a lawyer shall not knowingly “make a false statement of material fact or law to a tribunal.”

Although the Texas Disciplinary Rules do not prohibit a lawyer from searching for, extracting, or using metadata and do not require a lawyer to notify any person concerning metadata obtained from a document received, a lawyer who has reviewed metadata must not, through action or inaction, convey to any person or adjudicative body information that is misleading or false because the information conveyed does not take into account what the lawyer has learned from such metadata. For example, a Texas lawyer, in responding to a question, is not permitted to give an answer that would be truthful in the absence of metadata reviewed by the lawyer but that would be false or misleading when the lawyer's knowledge gained from the metadata is also considered.

Even though the Texas Ethics Committee did not go so far to impose a requirement that the receiving lawyer notify the sender, other jurisdictions have imposed such requirements. The New York State Bar Association concluded lawyers may not intentionally use computer technology to obtain privileged or other confidential information of an opposing party. The bars in Florida, Alabama, and Arizona have joined New York in holding that the recipient has a duty not to “mine” the document for metadata or otherwise engage in conduct amounting to an unjustified intrusion into the client-lawyer relationship existing between the producing party and the party's counsel. The District of Columbia Bar has declared a receiving lawyer is prohibited from reviewing metadata sent by an adversary only when the lawyer has actual knowledge that the metadata were sent inadvertently.

Be aware that sending electronic documents to another person may also result in the transmittal of metadata, and Texas attorneys have a duty to avoid the transmission of metadata containing confidential information.

d. Metadata: Discovery

Electronic discovery rules trend against the requirement that metadata be produced in discovery responses; however, a clear caveat is when the producing party is aware the metadata is relevant to the suit.[5]

Where system metadata is often relevant is if the authenticity of a document is questioned or if establishing who received what information and when is important to the claims or defenses of a party. Embedded metadata—such as “spreadsheet formulas, hidden columns, externally or internally linked files (such as sound files), hyperlinks, reference and fields, and database information”— can also be helpful in understanding electronic documents like complicated spreadsheets and, thus, are generally relevant and discoverable.[6]

Relevance of metadata and the relative significance to the case must be determined on a case-by-case basis. But metadata's relevance must be obvious or at least linked, more or less concretely, to a claim or defense. Hypothetical needs, surmise, and suspicion should be afforded no weight. Again, metadata may be necessary to the litigation when

[5] *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 652 (D. Kan. 2005).

[6] *Aguilar v. Immigration & Customs Enf't Div. of U.S. Dept. of Homeland Sec*., 255 F.R.D. 350, 355 (S.D.N.Y. 2008).

the who, what, where, when, and why electronically stored information was generated is an actual issue in the case, not merely a helpful or theoretical issue.[7]

While metadata may generally be discoverable, if relevant and unprivileged, that does not mean production in a metadata-friendly format is necessarily required. Whether production of metadata-accessible forms is required on demand engages the interplay between the discovery limits in Rule 192.4 and production of electronic discovery under Rule 196.4. That inquiry requires a balancing of the following factors: (1) likely benefit of the requested discovery, (2) the needs of the case, (3) the amount in controversy, (4) the parties' resources, (5) importance of the issues at stake in the litigation, (6) the importance of the proposed discovery in resolving the litigation, and (7) any other articulable factor bearing on proportionality.[8] Thus, metadata will be produced when relevant and when the factors above favor its production.

As an aside, when dealing with most any electronically stored information discovery issue, the Sedona Conference is a source of guidance to courts and parties. The Sedona Conference is a nonprofit legal policy research and education organization comprised of judges, attorneys, and electronic discovery experts dedicated to resolving electronic document production issues. Since 2003, the Conference has published a number of documents concerning electronically stored information, including the Sedona Principles. Courts have found the Sedona Principles instructive with respect to metadata issues. For more information and keeping up on latest trends on electronically stored information, the Sedona Conference is a great place to start.

e. <u>Metadata: Impact</u>

The emergence of metadata raises many issues, as seen in the most newsworthy metadata moment: the revelation that the U.S. government had been collecting bulk metadata on U.S. citizens. Bulk data and warrantless metadata collection—whether legal entities can collect or surveil metadata is one issue—but there are a number of metadata issues affecting the private sector too. Is there need for informed consent regarding collection? Is there clarity of use or sharing? Is there a need for expressed retention policy? How long can an entity store metadata?

Ultimately, the collection of your metadata is likely unavailable. Avoiding metadata collection is decidedly complex or exhausting, and it involves sacrificing the educational, social or business benefits that the Internet and the digital world has helped to deliver. Rather than seeking to avoid metadata collection, it is worth considering how to effect positive change in law and business practices, so metadata collection is beneficial and handled appropriately.[9]

III. THE CLOUD

a. <u>The Cloud: What is it?</u>

Cloud services are services made available to users on demand, via the Internet from a cloud computing provider’s server, as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider.

Cloud computing takes many forms. Cloud storage providers generally offer online access to shared computing resources with varying levels of functionality depending on the users’ requirements. Examples of cloud services include online data storage and backup solutions, Web-based e-mail services, hosted office suites and document collaboration services, database processing, managed technical support services and more.

b. <u>The Cloud: Security and HIPAA</u>

With the proliferation and widespread adoption of cloud computing solutions, HIPAA covered entities and business associates are questioning whether and how they can take advantage of cloud computing while complying with regulations protecting the privacy and security of electronic protected health information (ePHI).

[7] *In re State Farm Lloyds*, 520 S.W.3d 595, 607 (Tex. 2017)

[8] Tex. R. Civ. P. 192.4, 196.4.

[9] ICANN Blog, Author: Dave Piscitello, 27 Jun 2016.

The HIPAA Privacy, Security, and Breach Notification Rules (the HIPAA Rules) establish important protections for individually identifiable health information (called protected health information or PHI when created, received, maintained, or transmitted by a HIPAA covered entity or business associate), including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights with respect to their health information.

Covered entities (including law firms and lawyers that obtain PHI) must comply with the applicable provisions of the HIPAA Rules. When a covered entity engages the services of a cloud service provider to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the cloud service provider is a business associate under HIPAA. Further, when a business associate subcontracts with a cloud service provider to create, receive, maintain, or transmit ePHI on its behalf, the cloud service provider subcontractor itself is a business associate. This is true even if the cloud service provider processes or stores only encrypted ePHI and lacks an encryption key for the data. Lacking an encryption key does not exempt a cloud service provider from business associate status and obligations under the HIPAA Rules.

As a result, the covered entity and the cloud service provider must enter into a HIPAA-compliant business associate agreement (BAA), and the cloud service provider is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules.

c. Cloud-Based Services

Below are cloud-based services that meet HIPAA requirements:

Dropbox (Business): The company announced support of HIPAA and HITECH Act compliance in November 2015. It now provides BAAs for Dropbox Business customers. Administrative controls include review and removal of linked devices, user access, user activity reports, and enabling two-step authentication.

Box: Box added HIPAA/HITECH support in 2013. BAAs are provided for enterprise accounts. Features include access monitoring, reporting and audit trail for users and content, and granular file authorizations. Box integrations include Office 365, DocuSign, Salesforce, and Google, among others. It also allows for securely viewing DICOM files (for X-rays, CT scans and ultrasounds) and for securely sharing data through a direct messaging protocol.

Google Drive: Google offers a BAA for Google Apps for Work customers. Covered apps include Docs, Sheets, Slides, and Forms as well as several other services such as Gmail. (Some core and all non-core apps from the Google App family are excluded.) Administrative controls include account activity and app activity tracking, audits, and file-sharing permissions.

Microsoft OneDrive: Microsoft supports HIPAA/HITECH by offering BAAs for enterprise cloud services, and it has some of the best security practices in the industry. The security features are the most robust at the Enterprise E5 level. Enterprise E5 includes 1TB of file storage and sharing, advanced security management for assessing risk and gaining insights into threats and advance eDiscovery.

Carbonite: BAAs are provided for Carbonite for Office customers. Safeguards include offsite backup for disaster recovery, which the company says is widely accepted as the most stringent data protection in the country; and data encryption both in the cloud and on the local endpoint.

Egnyte: Egnyte's "enterprise" product is for businesses seeking HIPAA compliance. They are willing to sign a BAA. Egnyte delivers a comprehensive approach to security that offers complete control wherever files are stored. Total data protection at end points, in transit, and in storage. And universal visibility over all users and activities.

d. Office Use

Following are reasons lawyers are switching to and relying on cloud-based servers:

- Regular Updates: With cloud hosting and cloud storage, updates are done centrally and distributed to users.

- The Exchange of Electronic Data: Sharing documents with clients, counsel and others via the cloud makes the process simpler.

- Initial Lower Cost: While users spend a smaller fee at the beginning, they will continue to pay a regular monthly fee. However, it is unnecessary to upgrade hardware related to storage when using cloud storage, so the costs may balance out.

- Less Need to Worry About Disaster Recovery: Physical security and damage become far less worrisome for IT professionals when everything is stored in the cloud.

- Files Take Up Less Physical Space: With cloud storage, physical files can be converted and saved digitally without worry of competing for server space with active files.

- Accessibility: Files stored in the cloud are remotely accessible on a limitless number of platforms.

e. Client Use

Cloud servers allow professionals to securely share information with clients and for clients to do the same. Through cloud services, a client portal can be created through secure, client log in. It restricts access to only that client or invitee, where the client can view, download or upload documents, and send secure communications. The data is stored in the cloud and encrypted when transmitted. For solos, small firms, and boutiques this can be a very effective tool in improving client satisfaction.

f. Trial Use

With the continued growth in cloud-based platforms, sharing documents and evidence with the court and counsel during trial will move to the cloud. Many courts are already adopting cloud-based exhibit and document submission, and as cloud-based programs continue to meet heightened security demands, it is expected that electronic submission of evidence will continue.

IV. IDENTITY THEFT & CYBER SECURITY

a. Identity Theft: What is it?

“Identity theft” is the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit. The information can be used to obtain credit, tax refunds, merchandise and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, in rare cases, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

Identity theft typically occurs in one of two ways: (1) the thief uses personal information to open new accounts; or (2) the imposter uses personal information to gain access to the person's existing accounts. Within these two methods, there are many different examples of identity theft, such as:

- Tax-related identity theft, where a thief files a false tax return with the Internal Revenue Service (IRS) using a stolen Social Security number.

- Medical identity theft, where a thief steals information, including health insurance member numbers, to receive medical services. The victim's health insurance provider may get the fraudulent bills, which will be reflected in the victim's account as services they received.

- Child identity theft, where a child's Social Security number is misused to apply for government benefits, open bank accounts and other services. Children's information is often sought after by criminals, as the damage may go unnoticed for a long time.

- Senior identity theft, where a senior is the target of an identity thief. Seniors are often in contact with medical professionals and insurance providers, and may be used to giving out their personal information. They may also not be as aware of the scamming methods thieves use to steal their information.

b. Identity Theft Today and Your Clients

Although an identity thief might hack into a database to obtain personal information, it is still more likely the thief would obtain information by using old-fashioned methods. Retrieving personal paperwork and discarded mail from public trash dumpsters and the trash of businesses, is one of the easiest ways for an identity thief to get information. Recipients of preapproved credit card applications often discard them without shredding them first, leaving identity thieves free to attempt activating the cards and using them.

Phishing and spam email are used as methods of tricking people into offering up their information to identity thieves masquerading as legitimate financial entities, a colleague the recipient trusts or an individual who makes monetary promises in exchange for information. The email may contain attachments bearing malware designed to steal personal data or links to fraudulent websites where the person would be prompted to enter their information.

Here are some warning signs a person may be an identity theft victim:

- Victim notices withdrawals from their bank account that not made by them.
- Victim does not receive bills or other important pieces of mail containing sensitive information.
- Victim finds false accounts and charges on their credit report.
- Victim is rejected from a health plan because their medical records reflect a condition they do not have.
- Victim receives an Internal Revenue Service notification that another tax return was filed under their name.
- Victim is notified of a data breach at a company that stores their personal information.

Depending on the type of information stolen, the victim should contact the appropriate organization -- the bank, credit card company, health insurance provider or the IRS -- and inform them of the situation. The victim should request to have their account frozen or closed to prevent further charges, claims or actions taken by imposters. The identity theft victim should file a complaint with the Federal Trade Commission and inform one of the three major credit bureaus -- Equifax, Experian and TransUnion -- to have a fraud alert or account freeze placed on their credit records.[10]

Elderly clients are particularly vulnerable to identity theft. One of the main reasons is, they simply may be more trusting. In a study by the Massachusetts Institute of Technology, people were asked, “Do you feel that most people can be trusted?” So-called boomers, born 1946 to 1964, gave the highest percentage of “Yes” answers. The FBI notes that those who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting. Con artists, the FBI says, exploit these traits. A study at the University of California, Los Angeles, showed that older adults might have diminished “gut responses” to cues of untrustworthiness:

> “The elderly are prime targets for identity thieves because they are often easy to trick into providing personal information over the phone or in response to an email that can be used to make them victims of identity theft,” says Steven J.J. Weisman, Esq., a white-collar crime professor at Bentley University in Amherst, Massachusetts, and author of the book, ‘Identity Theft Alert.’”

Good credit and being generally wealthier than the generation before them also make elderly susceptible targets, as Forbes magazine reports.

The scams that identity thieves use to target seniors are similar to the ones used to target other victims, as discussed above. Among them:

[10] Margaret Rouse, TechTarget, April 2017.

- Telephone scams: Identity thieves target seniors over the telephone, looking to gain their trust to gain personal and financial data that can be used to commit fraud. As noted above, thieves can pretend to be a person in authority to solicit information, and they may employ a sense of urgency that prompts the victim to move quickly, without taking time to think about the consequences.

- Internet scams: Online con artists often "phish" for personal data through email, transmitting seemingly legitimate requests that claim information is needed by the senior victim's bank, credit card, or mortgage company. The criminals may ask seniors to verify their financial data (like account numbers and Social Security numbers). Security service Lifelock reports that over 90 percent of all reported elder abuse is committed by the older person's own family, most often by their adult children. Make sure those you trust are trustworthy.

What can clients and consumers do to protect themselves? While no plan will guarantee 100% security, clients should also consider the following courses of action:

- Check Accounts Regularly – Frequently review all credit and debit card accounts for unknown purchases that could indicate fraudulent use.

- Consider a Monitoring/Prevention Service – Services are available to monitor your credit report for suspicious behavior and make it difficult for thieves to open false accounts in your name.

- Use Strong Passwords – Find passwords that have meaning to you but are difficult to hack.

- Protect Your Passwords – Do not save passwords on your computer or let your computer remember passwords.

- Avoid Password Duplication – Use unique passwords for each account.

- Keep Devices Protected – Make sure that your computer, smartphone, and other devices that are connected to the Internet have the latest protections. Update protection software regularly and check the news for any new threats that require immediate updates. Use file encryption whenever possible to protect individual files in case your system is breached.

- Use Secure Wi-Fi – Unsecured wireless Internet connections can thwart all of your other protections.

- Use Multi-Factor Authentication – Take advantage of multi-factor authentication when it's available. Typically, this involves a secondary temporary security code that is sent via e-mail or text message. The code must be entered before a transaction is completed.

- Dispute Errors – Immediately address any mistakes or false charges on credit cards or debit cards, no matter how small. They could be the first sign of a breach.

- Cancel Compromised Accounts – Cancel any compromised debit or credit accounts and replace them with new cards as soon as possible – but make sure banks and credit card issuers are aware of the situation to avoid missed payments and penalties during the transition.

- Set Up Alerts – Many cards have fraud protections and alerts to notify you of questionable charges, odd purchasing patterns, or unusually large purchases. Take advantage of any program that is offered, and consider switching to a different card if your current one does not offer protections.

- Shred Old Documents –Shred any documents, even junk mail, that contains information useful to thieves – and consider a locking mailbox to avoid mail theft.

- Review Medical Statements – Medical claims are confusing and take a long time to process. A fraudulent medical claim in your name could reach collections before you even know it exists. Look for Explanations of Benefits (EOBs) for unfamiliar groups or procedures.

- Stick With Trusted Sites – Stay with familiar websites and be suspicious of any external links. Look for "https" in your browser window, as the "s" indicates a secure site – but even this system is not foolproof.

- Stay Familiar With Scams – Phishing e-mails and fake websites are becoming more elaborate and difficult to discern. Note any new scams that are reported, and trust your instincts if you find a new e-mail or text message that looks suspicious.

- Confirm Links – If you receive a link an email of someone you know but are not expecting, confirm with the sender that they in-fact sent the link before opening.

Again, these steps will not guarantee success against identity theft, but they decrease vulnerability by making yourself or your client a difficult target.

c. <u>Cyber Security at the Office</u>

Data breaches are becoming commonplace in the legal field, as the frequency of attempts and attacks has been increasing substantially. Law firms are very attractive targets. They have information from clients on deal negotiations which adversaries have a keen interest in," according to Harvey Rishikof, co-chair of the American Bar Association's Cybersecurity Legal Task Force. "They're a treasure trove that is extremely attractive to criminals, foreign governments, adversaries and intelligence entities."

Cisco Systems Inc. ranks law firms as the seventh most-vulnerable industry to "malware encounters" in its 2015 "Annual Security Report," other statistics are more striking. Most problems stem from a lawyer or staff-member who clicks on a fake e-mail. These e-mails can range from the easy-to-spot fake to the more elaborate hoaxes and impersonations.

It is important that law offices have an information security policy that covers all information systems, including: e-mail, voicemail, text messages, the Internet, computers, work stations, laptops, cell phones, software, passwords, remote access, and cloud computing. Creating an office-culture where awareness of these risks is known top-to-bottom will help avoid breaches and allow for faster identification and recovery when the breach occurs…which IT WILL. Quantifying the risks: a mid-size firm should expect approximately 20,000 "Brute Force" attempts against Remote Services (Terminal Server) and about 10 "Phishing Attempts" via e-mail per day.

Below are some "best practices" to curtail risk:

- A password and idle time-out of no longer than three minutes is required on all portable-computing devices that store Personal Health information or other confidential data, including email, whether or not the hardware is owned by employee; this includes personal devices (phones, tablets, etc.).

- Portable computing devices that have stored data belonging to the firm (including firm email), may not be shared with others who are not authorized to access that information unless that information is stored as encrypted password protected files.

- Portable computing devices must be protected at all times. This includes but is not limited to, not leaving it in plain sight in cars, trains, hotel rooms, at home, restaurants, etc.

- Access to firm systems and network remotely must first be approved by the department supervisor and the Information Technology Department.

- Access to the firm's internal network from outside of its defined network perimeter must be controlled by privileged access controls that may only be established by the Information Technology Department.

- Conducting business on public computers and unsecure Wi-Fi is not allowed, such as cafes, hotels, libraries, airport, etc.; employees should turn off the Wi-Fi feature on smartphone/tablet devices to prevent unsecured Wi-Fi access on their devices.

- The loss or theft of any portable computing device on which firm client data or sensitive business information (including firm email) is stored shall be immediately reported to Department Supervisor whether or not the firm owns the hardware.

For more practical security tips, see the ABA Journal article: Preventing Law Firm Data Breaches, Volume 38 Number 1, Law Practice Magazine 2012. See also Ellen Rosen, Most Big Firms Have Had Some Hacking: Business of Law, Bloomberg Business, March 10, 2015.

As lawyers and paralegals plunge further into mobile and smart devices, it will become a necessity that attorneys and staff bring their own devices to work. With an increased number of personal devices being capable of replacing the traditional workplace, legal professionals need to understand the risks of the bring your own device (BYOD) trend and should have policies in place to curb the risk associated with BYOD.

The biggest risks in BYOD are data breach and loss. An effective BYOD policy should address behaviors and activities allowed on personal devices and what information is accessible on such devices. Because most practitioners do not have access to resources or infrastructure to protect and secure all data on their networks, Mobile Device Management services could be used to equip law offices with tools and security to protect devices and data. These services may include software that allows encryption of data on mobile devices, knowing location of devices in real time, enforcing a PIN policy, access of personal data and contacts, and tracking user activity. At a minimum, attorneys should have a policy that all mobile devices be password protected.

With any security policy, risk management and privacy are often competing interests. Attorneys must be conscience that their BYOD policy or security services could infringe on employee privacy. Precise, transparent guidelines for protecting firm data should be made available to all employees, and consent from employees to monitor their devices should be acquired to have a successful BYOD policy.

Mobile and smart devices have enormous upsides in providing lawyers the ability to practice and be accessible to their clients nearly anywhere. But lawyers must be cognizant of the risks of other attorneys and staff integrated their personal devices into the workplace. Being aware of these downsides, putting policies in place to curb risk, and reviewing those policies regularly can help eliminate BYOD problems.

Being HIPAA compliant also requires attorneys to take numerous security steps, including:

- Physical Safeguards: Law firms must make sure their networks, data and offices are physically secure. This means that firms need to make sure that only people who are authorized and trained on HIPAA can access servers and data. This extends to computers and tablets.

- Technical Safeguards: Sensitive data needs to be secured with encryption, passwords and other methods. If firms are not already doing so, they need to monitor activity on systems that hold protected data.

- Administrative Safeguards: Firms must have methodologies for preventing, detecting, containing and correcting security violations. That involves naming a security official and ensuring that attorneys and staff are trained annually on their responsibilities. Firms also need to develop plans to identify, respond to, mitigate and document security incidents. They must create emergency response procedures to secure data backup and recovery to account for any potential disruption from a natural disaster to an accidental or deliberate data breach. If a data breach occurs, all business associates, including law firms, need to follow the guidelines that are outlined in their HIPAA policies and procedures on disclosing the breach.

With HIPAA's compliance requirements, firms need a resource (either in-house or outsourced) that possesses in-depth familiarity with the regulation and experience with successful HIPAA audits in compliant organizations. If firms don't know what HIPAA goals they need to achieve, they run the risk of noncompliance.