CLM National Conference
March 14 through March 16, 2018
Houston, Texas

RISK MANAGEMENT FOR CLIENT CONFIDENTIALITY IN THE DIGITAL AGE

I. Vigilance Is The Price Of The Digital Age:

As long as there is opportunity there will be enterprise. Through the 1990s, the information age was born. It has taken hold. It has made the world smaller. It has put the latest news in the palm of your hand within minutes, if not seconds. We have become accustomed to this convenience, perhaps taking it all for granted-especially in its absence. In this world of remote access to instant information comes the blessings of its convenience and the burden of new risk. Vigilance, a time honored watchword, is the price of this new age.

Vigilance is both pro-active and reactive. In the pro-active sense, it is all the steps and measures taken to design, create and perpetually update the wireless, paperless world. From our homes, cars and yes, vacation destinations, the access to our work is now 24/7. This enhances productivity, elevates customer service and raises the bar of achievement.

Yet no system is impervious to attack. The pro-active includes anti-virus software, encryption, backup systems, password protection are among at least some of the steps considered for any digitally based information system. This is not enough. Reactive steps are already in place. Cyber insurance once thought fanciful is more common. Planning for a breach, response teams, notification protocols, system checks with even the most trusted vendors are the norm, not the exception.

The pickpocket's New Year's Eve is the cyber criminal's daily routine. A world full of wireless online activity moving information, money, medical data, confidences and tomorrow's news is ripe for the harvest today. New words and phrases together with new meaning for old ones has permeated our vocabulary: phishing, ransom ware, hacking, data breach, botnet, cyber infrastructure, electronic signature, malware, spyware, dark web and bitcoin.

This panel examines confidentiality in the digital age as an imperative against cyber theft. At stake are the fundamental principles between attorney and client; between insurer and its insured, between third party administrator and attorneys, insurers and their insureds alike.

II. A Reminder Of The Rules Of The Road:

A. Law Firms:

The vast majority of states follow the American Bar Association (ABA) Model Rules. In ABA Rule 1.6(a) and (c) it states:

> "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent ….
>
> ***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."*** (emphasis added).

In Texas, this protection of confidentiality extends even to those situations where a client posts a negative review on the internet. In interpreting Rule 1.05 of the Texas Disciplinary Rules of Professional Conduct does not allow the lawyer to use confidential information in a response. (Opinion 662, The Professional Ethics Committee For The State Bar of Texas, August, 2016). Thus, if you cannot defend yourself against a negative review from a client despite what you know from them, then, certainly the duty to preserve the confidentiality of that client's confidential information from cyberattack is imperative.

While Texas has not yet adopted ABA Model Rule 1.6 (c), commentators have referenced the need for law firms in Texas, and elsewhere, to safeguard against cyberattack. "Recognizing the Increasing Risk of Cyber Attacks," by Shari Klevens and Alanna Clair, Texas Lawyer,October 26, 2017. The authors noted that law firms with 100 or more lawyers had a 25% rate of a data breach. These may arise from lost equipment, stolen cell phones and website attacks. Further, they noted that hackers view law firms as soft targets that represent multiple opportunities to leverage both client and the firm's own information.

Even DLA Piper, one of the leading law firms in the world, who has an impeccable reputation for security, was subject to cyberattack in mid-2017 requiring extraordinary measures in response.

Law firms possess not only confidential client information, but identifiers such as social security numbers, medical information, trade secrets, intellectual property, trust accounts with money, and prospective transactional and litigation strategies. As Courts have permitted suits against companies who possess sensitive financial information in the ordinary course of business, it is not unlikely that they will also do so with law firms triggering a new challenge and risk.

As law firms typically need to "…keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology..," ABA Model Rule 1.1 Comment, the correlative duty to safeguard client confidential information becomes paramount. As the breach may give rise to a claim for malpractice, notification to the client will be required. As such, the requirement of security measures to protect against cyberattack become paramount. Restatement (Third) of the Law Governing Lawyers, Section 20, Comment C (American Law Institute, 2000).

B. <u>Insurers:</u>

Sadly, insurers have also been the victims of cyberattack. Health insurers, like Anthem Blue Cross, which possesses incredibly confidential medical and personal information, have been the subject of such attack. Not only are identifiers present, such as social security numbers and other personal information, but also the medical identity of their insured patients.

The National Association of Insurance Commissioners (NAIC), Center for Insurance Policy and Research, have focused on cyber security by creating a working group with the focus on insurance regulatory activity related to cyberattack. The information sought focuses on security programs for ongoing risk assessment, oversight of third party service providers and developing a series of common steps in the event of data breach. The NAIC has already developed several publications available on its web based information including:

1. Roadmap for Cybersecurity Consumer Protections; and,
2. Principles for Effective Cybersecurity: Insurance Regulatory Guidance.

(NAIC, The Center for Insurance and Policy Research, "Cybersecurity," October 31, 2017). Principles include, in summary, the following:

1. State insurance regulators have responsibility to ensure security of personal information held by insurers;
2. Confidential information collected, stored or transferred inside or outside insurers databases shall be safeguarded;
3. State regulators have the obligation to protect information provided to them by insurers and/or NAIC;
4. Cybersecurity regulatory guidance for insurers and their producers must be scalable, practical and consistent with efforts by the National Institute of Standards and Technology;
5. Regulatory guidance must be risk based, consider resources with the caveat that linkage to the internet requires minimum cybersecurity standards regardless of company size;
6. State insurance regulators shall conduct regulatory oversight, risk based financial examination and market condition cybersecurity;
7. Planning for incident response by insurers, their producers and other regulated entities is essential to cybersecurity;
8. Insurers should take appropriate steps to ensure that third party service providers protect personally identifiable information;
9. Cybersecurity should be incorporated into an insurer or insurer's producers ERM model as cybersecurity transcends all facets of the operation;
10. Information technology interval audits should be reviewed with the insurers board of directors or designated committee;
11. Insurers must use information sharing and analysis organization (ISAO) to say abreast on recent trends and emerging risks; and,
12. Periodic training of insurer, insurer producer, third party and service providers personnel on cyber security is essential.

3. Third Party Administrators:

A Third Party Administrator (TPA) processes insurance claims or employee benefit plans for its clientele. In California, third party claim administrators are required to hold requisite licenses, complete continuing education and comply with the general requirements applicable to their clientele. TPAs are generally not parties to a contract of insurance. Thus, some jurisdictions, focusing on privity of contract, hold that a TPA cannot be held liable as the insurer. For example, the Supreme Court of California decided that no colorable claim existed against the third party administrator in Gruenberg v. Aetna Insurance Company (1973) 9 Cal. 3rd 566.

The modern trend is to hold TPAs accountable not based on an insurance contract, but based on a general duty of care for the principal objects of their adjustment. Thus, the United States District Court for the Southern District of Ohio, noting trends from other states such as Alaska, New Hampshire and Oklahoma, held that there is a duty of care applying to the insured and those affected foreseeably by their decisions. Shephard v. Allstate Insurance 2006 U.S. Lexis 563 (S.D Ohio, 2006). A variety of recent decisions focusing on conduct, rather than direct privity, have followed. Further, with the advent of contractual indemnity which broadly transfers the potential defense and indemnification arising out of or related to their scope of professional services (see Crawford v. Weather Shield Manufacturing (2008) 44 Cal. 4th 541), it follows that a TPA is unlikely to escape legal responsibility for data breach.

4. Federal Law:

The Cybersecurity Information Sharing Act of 2015 recognized that a collaborative model of sharing threat and risk information between the private sector and the Federal government is essential in combating cyberattacks. President Trump executed an Executive Order on May 11, 2017, focusing the executive departments to strengthen and coordinate defenses to potential cyberattacks. Further, on November 30, 2017, Elaine Duke, Acting Secretary for the Department of Homeland Security, noted that there are world-wide threats which represent a form of terrorism against the United States. Thus, with both private actors hacking for profit and state sponsored actors using digital means against our national security interests, the theatre for and means of cyberattacks is only likely to grow.

5. State Law:

In 2016, several states have adopted cybersecurity related laws such as: California (A.B. 1841, A.B. 2623, S.B. 725), Colorado (H.B. 1453), Delaware (S.B. 258), Florida (H.B. 1025, H.B. 1033, S.B. 624) Georgia (S.R. 360, S.R. 412), Indiana (H.R. 2), Kansas (H.B. 2442), Maryland (H.B. 1168), New Hampshire (S.B. 406), New York (S.B. 7601), Oregon (S.B. 1538), Utah (H.B. 241 and S.B. 183), Virginia (H.B. 817, H.B. 1343, and S.B. 494), Washington (H.B. 2375 and S.B. 6528) and Wyoming (Chap. 35). In general, these laws identify cyber security as an issue such as defining a crime, funding research and advisement, requiring certain agencies to act and refining public records responses to avoid inadvertent disclosures.

An equal number of states considered, but adjourned without enacting such legislation. It is obvious that the insurance industry will be next as it possesses so much information desirable

and subject to cyberattack. (National Committee of State Legislatures, "Cybersecurity Legislation 2016," December 8, 2016). More states are expected to adopt laws in 2017. The results for 2017 will be reviewed and summarized as many are still under consideration for approval.

A variety of states have enacted more detailed legislation covering all business entities and individuals, such as Florida. Governor Rick Scott signed into law the Florida Information Protection Act of 2014 (S.B. 1524). Further, in Florida, The Florida Cyber-Security Manual, "C-SAFE 1.1, " published by the Florida Department of Law Enforcement, provides over 300 pages of information on definition of cybersecurity terms, situational awareness, pro-active measures response procedures and training protocols. Training publications, such as these, are, together with NAIC research and standards, source materials for insurers, insurance producers, third party and their vendors.

III. Confidentiality For Lawyers, Insurers and TPAs:

A. Planning:

With the assistance of expertise in digital security consultation, law firms, insurers, TPAs and their vendors have to plan to succeed. As we meet in Houston, home of NASA, we are reminded of a phrase of Flight Director Gene Kranz during Apollo 13: ***"… failure is not an option."***

B. General Issues to Consider:

A variety of plans, steps and considerations may apply to any firm, insurer, TPA or vendor; however let's stick with the Top 10 overall issues:

1. Use of Wi-Fi in public places;
2. Type and use of portable technology;
3. Privacy practices including controlling access;
4. Security measures for sensitive data;
5. Integration of best practices throughout the organization;
6. Screening of employees and those with access to confidential information;
7. Establishing routine review of systems, updates and security;
8. Disseminating information to all employees and users of network systems;
9. Initiation and updates on training for all employee and users for network systems; and,
10. Maintaining vigilance for all systems, sensitivity to trends and updated information.

IV. Looking Forward For Law Firms, Insurers, TPAs and Their Vendors:

First, from an underwriting standpoint, law firms will be asked about cybersecurity and their data management profiles. Second, given the probability of cyberattacks, the consideration for and placement of cyber insurance will become more commonplace for all stakeholders. The interplay of insurance coverage potentially applicable to cyber risk will become more refined as the development of free standing policies continues to evolve.

At present, potential for coverage may exist for cyber events under a variety of policies: cyber insurance, errors and omissions, fidelity coverage, general liability, directors and officers,

employment practices liability and umbrella coverage. Each presents a different aspect, but key will be initial response after a data breach (securement of system, identification of lost information, notification and response). While liability coverage for third party claims is highly desirable, without an effective, comprehensive initial response, the benefits of third party coverage may amount to a pyrrhic victory in the wake of business collapse.

Insurers and TPAs will require of their law firms, third parties and vendors, assurance that this risk has been fully considered, security systems are already in place and pro-actively updated and that cyber coverage exists to assist in early response to a data breach. Frankly, in the absence of that type of assurance, business will be restricted to those who do.

V. Conclusion:

At the time of writing this article, UBER has been accused of covering up a massive data breach. In Congress, several legislators have re-introduced the Data Security and Breach Notification Act previously introduced by Florida Senator Bill Nelson. The commonplace nature of data breach, the alleged efforts of some to cover up the consequences and ever present threat serve as a solemn reminder that this risk falls squarely on lawyers, insurers, TPAs and their vendors.

We live in an information age whose advancement of technology has outstripped our humanity and left many institutions vulnerable to cyberattack. The stakeholders in this community, from insurers to their TPAs to counsel to third parties to vendors, are intertwined with overlapping responsibilities to maintain and secure client confidentiality. Confidentiality is not simply an operative safeguard to handling a case or claim; it is a duty to ensure that the information entrusted to this process remains secure to protect all stakeholders effectively. Failure is not an option.

Respectfully submitted,

Howard Franco, Jr.
Caryn Siebert
Dustin Sachs
Frank English