2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

"WAITING FOR THE OTHER SHOE TO FALL"

CIVIL CLAIMS AGAINST PROFESSIONALS FOLLOWING DATA BREACH

Lawyers and other professionals increasingly practice in a virtual world. Professionals communicate with their clients, adversaries, the government and the Court through electronic means, negotiate and conclude transactions on shared Internet portals, conduct meetings in virtual meeting places and even store their business records and files, electronically, both on and off-site. The "virtual office" is no longer at the cutting edge. The new outlier is the practitioner that does not make use of these virtual tools.

And with these tools, come additional risks of data breach. Lawyers as well as accountants and medical professionals in particular receive a great deal of information that is potentially attractive to cyber thieves. Moreover, the type of data maintained by professionals is rich. Whether as to clients or employees, professionals maintain a treasure trove of protected health information ("PHI"), personally identifiable information ("PII"), private and/or confidential information. Social security numbers, identifying information, account numbers, medical insurance, health records and proprietary confidential business plans may all reside in the professionals' "virtual office" and therefore be vulnerable to breach.

Indeed, some reports estimate that 80 out of the 100 largest law firms have been hacked as of 2011.[1] The risk, however, is not limited to large firms. Since 2009, at least, the FBI, secret service and law enforcement have warned that law firms are among the most high risk targets. In identifying the growing risk of data breach that accompanies increased technology dependence, the FBI stated that "[t]he more mobility you have, the more documents you're sending through the internet, the more likely you are to be the victim of a cyberattack…"[2] Plainly, the professional practicing in the "virtual office" environment is at the pinnacle of such mobility.

Ethical Obligations

In recent years, there has been a flurry of ethics opinions in numerous states across the country that discuss attorneys' ethical obligations to preserve and protect confidential information that is obtained in the course of legal practice, when using technology, such as "cloud computing," or other similar online backup and file storage devices.[3] These technologies are at the core of professionals' ability to conduct a virtual practice and the ethical problems they may have if a cyber breach occurs.

The general consensus is that lawyers have a duty to understand the technology they employ, and to take reasonable measures to protect confidential information. By reason of his/her exclusive or increased reliance on technology to provide legal services, the virtual practitioner has the same or greater obligations to take reasonable efforts to secure their

[1] *See e.g.*, Hansen, *Cyber Atacks Upend Attorney-Client Privilege* available at http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security

[2] *See* Koblentz, *LegalTech Day Three: FBI Security Expert Urges Law Firm Caution*, Law Technology News, available at http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202586539710&LegalTech_Day_Three_FBI_Security_Expert_Urges_Law_Firm_Caution.

[3] A survey of such ethics opinions, by state, is available on the ABA's website at, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

clients' data from unauthorized access when the data is in transit to the attorney's internet portal, maintained in the attorney's virtual file or in the control of an attorney's outside vendor.

In August of 2012, the ABA approved a number of technology-related changes to the Model Rules of Professional Conduct ("Model Rules").[4] As may be particularly relevant to addressing the higher technological dependency of the virtual practitioner, Rule 1.6 (pertaining to client confidentiality) was amended to add a new section (subsection "c"), which requires that lawyers make "**reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.**"[5] Comment [16] to Rule 1.6 was also amended in order to make clear that "reasonable" efforts by the attorney to protect client information will be considered an element of "competency" for purposes of Rule 1.6, even if unintentional disclosure does occur, and now provides a non-exclusive list of factors to consider in determining what was reasonable. In addition, Comment [16] recognizes that some clients may require the lawyer to implement special security measures not required by the Rule or may give informed consent to the use of security measures that would otherwise be prohibited by the Rule. Comment [16] also provides a final caution -- compliance with Rule 1.6 does not vitiate attorneys' obligations under federal and state law regarding privacy and/or notice requirements in the event of a privacy breach.

A series of smaller, but key changes were also adopted to address confidentiality concerns. For example, Comment [6] to Rule 1.1 (concerning attorney competency) was amended to add the underlined language: "lawyers need to keep abreast of changes in the

[4] *See e.g.*, Lewis, *ABA Approves Changes to Technology Related Ethics*, N.Y.L.J. Aug. 14, 2012, available at http://www.rivkinradler.com/publications.cfm?id=996.

[5] The ABA Model Rules can be found at, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.

law and its practice, including the benefits and risks associated with technology . . . ." Additionally, Part (b) of Rule 4.4 (Respect for Rights of Third Persons), which addresses the particular ethical issues associated with the inadvertent disclosure of confidential information, was amended to apply not only to "documents," but also to "electronically stored information."

Statutory and Common Law Obligations

Defining the scope of the legal practitioner's ethical obligations when it comes to cyber breach is complicated by the extra-territorial nature of "virtual" practice as specific duties may vary from state to state and depend on fact specific inquiries as to the nature of the representation and the sensitivity of the information that has been entrusted to the professional. Various federal and state statutes and regulations require the protection of specific categories of client and non-client personally identifiable information and many of those statutes likely apply to attorneys who come into possession, transmit or store such personal information through internet enabled applications. For example, professionals are increasingly likely to come into possession of social security numbers, driver's license numbers, state-issued identification card numbers, bank account numbers, credit card numbers and certain health information regarding their clients, third parties and non-clients and even their "virtual" employees that operate in locations that may be in other jurisdictions than where the professional is located.

In addition to professional standards that may compel additional action, as of October 2015, 47 states, the District of Columbia, Puerto Rico and Virgin Islands have each enacted their own version of data breach notification statutes, which vary widely as to when, how and

to whom notification must be sent.[6] There is, however, still no uniform federal guideline as to breach notification in the case of multi-state involvement.[7]

Additionally, the scope of common law privacy tort law varies greatly from state to state. For example, some states permit a tort action for invasion of privacy in all circumstances or, in limited circumstances, like when PHI is involved. Other states do not recognize any common law tort claim for invasion of privacy, except against specific categories of professionals, (i.e. doctors) in regard to specific types of information. [8] Moreover, many common defenses to cyber breach tort claims – such as the ability to establish standing or damages – are being eroded as more and more cyber breaches occur. [9]

How to Ameliorate the Risk

Unlike traditional law office practice, despite the proliferation of security programs, in the virtual law office there is still no fail safe way to simply lock the file cabinet that contains confidential or personal information in the lawyer's possession to prevent unauthorized intrusion. It is intrinsic to the conduct of the virtual law office that such confidential data will be transmitted among several computers and stored in servers that are almost certainly not

[6] *See* National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx; . *see also*, Goodman, *Your Duty if You Discover a Data Breach,* ABA Solo, Small Firm and General Practice, available at http://www.americanbar.org/content/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/databreach.html.

[7] *See* Ponemon Institute, 2014 *Cost of Data Breach Study: United States*, available at. http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis According to Ponemon, the average cost to a company was $3.5 million in US dollars and 15 percent more than what it cost the year prior.

[8] See Lewis and Gershonoff, *A Landscape View of Privacy Protection Issues* available at http://www.rivkinradler.com/publications.cfm?id=999

[9] *See*, *e,g*, .Lewis, *Standing to Assert Claims for Online Privacy Breaches*, December 15, 2015 available at https://www.rivkinradler.com/publications.cfm?id=1833

under the attorney's control. The fundamental nature of the virtual office presents numerous occasions for data to be improperly accessed, adulterated or lost, either in individual matters or as the result of a concerted effort to breach the virtual office's security.

Notably, because increasingly, most if not all data is stored electronically, all professionals operating a virtual office may have greater exposure if vulnerable information is, in fact, stolen. Although attorneys have not been in the forefront of reported data breach cases, it would be foolhardy to consider any profession to be risk free. For example, since 2009, the FBI has issued repeated warnings that law firms are the intended targets of many data theft schemes.[10]

To allay some of this risk, the Minimum Requirements proposed by the ABA's e-Lawyering Taskforce suggested the following steps be undertaken to protect client confidences:

> 1. **Encryption:** All data that is transferred online between the law firm's web site and the server must be encrypted.
>
> 2. **Third-party hosting providers.** The Taskforce recommended that the lawyer providing internet enabled services vet third-party hosting providers to ensure that the provider has policies and procedures in place a) to protect against security breaches, data theft, and protect privacy; b) outline under what circumstances the third party provider's staff is permitted to access client data, and that when they do so for technical reasons they are acting as agents of the law firm; and c) that the procedure guarantees the security of the firm's client data, provides for redundant back up and a process for exporting the data at the firm's request.
>
> 3. **Security Certificates.** The Taskforce also recommended that virtual practitioners consider securing various certifications that confirm the security and the privacy policy of the web sites in order to provide notice to their clients that the secure portions of the website comply with industry standards for security.

Insurance Issues

---

[10] **See *Simek and Nelson,* Preventing Law Firm Data Breaches, *ABA Law Prac. Vol. 38, No. 1, available at*** http://www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html.

There is little doubt that the virtual professional officeoffer both great opportunities and challenges to determine what insurance is needed by the professional and address the challenges of underwriting those risks. Some of the factors that complicate that risk assessment are:

1) The "law without boundaries" potential geographic reach of virtual practice;

2) The unintended consequences of representation, especially if offered in an "unbundled" setting or in areas where the attorney may not be familiar;

3) The possibility of unintended attorney responsibilities in jurisdictions where direct retention and privity have been eroded;

4) The difficulty in assessing remote professional participants in the representation, such as where different parts of the representation are handled by different remote participants in the virtual endeavor;

5) The reliance on vendors, such as third party servers, software as service providers, internet service providers, cloud servers, etc. and their individual guarantees, warrantees and insurance or resources for indemnification in case of breach;

6) The unsettled nature of the law regarding the virtual office as a paradigm for providing legal services which is well out paced by practitioners' adoption of that paradigm.

Nevertheless, neither practitioners nor insurers are without guidance. For example, lawyer professional liability policies are frequently issued only after careful examination is made of the nature of the practice. Technology use in the practice, as well as third party vendor contracts, will probably be an increasingly important part of that examination in the future.

It is noteworthy that whereas most lawyer professional liability policies provide coverage when a claim is made in connection with the provision of professional services, some expressly exclude liabilities that arise from the use of the internet and other cyber exposures. It

will be interesting to see the interplay of these two common insurance policy terms, particularly where a claim is made as a result of a cyber breach that grows from confidential client information and in light of the increasing technological competence that attorneys are expected to use in their practices.

Additional coverage cyber for non-typical liability claims is now often offered to supplement or allay defense costs in connection with ethics grievances. However, as demonstrated by the advisory, qualified nature of the ABA e-Lawyering Taskforce report, the lack of predictable ethical standards regarding virtual law office practice could make even the most careful lawyer susceptible to an ethical problem. As such, it may be difficult to assess and underwrite that risk when providing coverage to virtual law office practices.

Another type of valuable insurance that the professional practicing in the virtual office may wish to explore is cyber coverage, which is designed to provide first and, if necessary, third party benefit in the event of data breach. The cost, inconvenience and damage to one's reputation as a result of a data breach can be stunning. Cyber coverage generally offers coverage not just for third party claims, but for first party notice as may be required under the various statutes.

In sum, it is important that the insurer and practitioner assess the likelihood that certain risks will shift in response to greater technological reliance and provide appropriate coverage as well as knowledgeable defense of claims should novel claims arise in the context of virtual professional practice.