Law Firm Data Breaches: The Cone of Silence Shatters

By Sharon D. Nelson, Esq. and John W. Simek

For years, the authors (and many others) have been saying that law firms generally keep mum about data breaches. While we have seen a few small firms abide by data breach notification laws, the larger firms generally have not, usually hanging their hat on the "we don't know what data was compromised" or the "we had an incident, but no evidence of an actual breach or misuse of data" excuses. In fairness, not all data breach notification laws are equal – in some cases, they may not have to disclose Whether they have told their clients is unknown, but speculation has been rising that they often have not, for fear of a mass client exodus.

Two Am Law 100 Firm's Breaches Announced

The "Cone of Silence" around law firm data breaches began to shatter on March 29, 2016, when the *Wall Street Journal* reported that Cravath Swaine and Weil Gotshal, two members of the Am Law 100, were breached in the summer of 2015. Other firms, not named, were reportedly breached as well.

The Manhattan U.S. attorney's office and the FBI are probing the breaches. It isn't clear what information may have been compromised. The information in the article came from "people familiar with the matter." Because the story came from the *Wall Street Journal*, we are quite confident that they verified the information.

Cravath acknowledged that there was a "limited breach" but said that the firm is "not aware that any of the information that may have been accessed has been used improperly." The firm said it was working with law enforcement and outside consultants to assess its security. A spokeswoman for Weil Gotshal declined to comment.

Declining to comment is not a security strategy but it sure has been used as one in the legal world, where breaches are off the record, on the QT and very hush-hush. We bore witness to this when we were once invited, as digital forensics experts, to a very elite meeting of law firm CIOs who didn't mind admitting breaches

amongst themselves, but we were sworn to silence, even forbidden to mention the firms represented in the meeting.

Russian Cybercriminal Targets Major Law Firms, Seeks Hacker Partner

March 29th was a tough day in the legal world. Not only did the *Wall Street Journal* publish its article on the breach of two Am Law 100 firms, but *Crain's Chicago Business* reported that a Russian cybercriminal called "Oleras," living in the Ukraine, had been trying since January 2016 to hire hackers to break into the computer networks of nearly 50 elite law firms (almost all U.S. firms) so he could trade on insider information. The source of the story was a February 3rd alert from Flashpoint, a New York threat intelligence firm.

Oleras posted on a cybercriminal forum that he planned, once the law firms were compromised, to use keywords to locate drafts of merger agreements, letters of intent, confidentiality agreements and share purchase agreements. His list of targeted law firms included names, e-mail addresses and social media accounts for specific law firm employees.

Oleras hoped to hire a black-hat hacker to handle the technical part of breaking into the law firms, offering to pay $100,000, plus another 45,000 rubles (about $564). He offered to split the proceeds of any insider trading 50-50 after the first $1,000,000. Sporting of him.

On February 22nd, another Flashpoint alert said that Oleras had singled out eight lawyers from top firms for a sophisticated phishing attack. The phishing e-mail appeared to come from an assistant at trade journal *Business Worldwide* and asked to profile the lawyer for excellence in mergers and acquisitions.

The firms targeted reads like an entry from Who's Who Among Law Firms. Targets included Akin Gump, Allen & Overy, Baker & Hostetler, Baker Botts, Cadwalader Wickersham & Taft, Cleary Gottlieb, Covington & Burling, Cravath Swaine (which we now know suffered a breach last summer), Davis Polk, Debevoise & Plimpton, Dechert, DLA Piper, Ellenoff Grossman, Freshfields Bruckhaus, Fried Frank, Gibson Dunn, Goodwin Procter, Hogan Lovells, Hughes Hubbard, Jenner & Block, Jones Day, Kaye Scholer, Kirkland & Ellis, Kramer Levin, Latham & Watkins, McDermott Will & Emery, Milbank Tweed, Morgan Lewis, Morrison & Foerster, Nixon Peabody, Paul Hastings, Paul Weiss, Pillsbury Winthrop, Proskauer Rose, Ropes &

Gray, Schulte Roth, Seward & Kissel, Shearman & Sterling, Sidley Austin, Simpson Thacher, Skadden Arps, Sullivan & Cromwell, Vinson & Elkins, Wachtell Lipton, Weil Gotshal (which also suffered a breach last summer), White & Case and Wilkie Farr.

Why list the firms? First, because smaller firms express skepticism about threats to law firms in general. This is a wake-up call. Second, because there is no secret about which firms hold M&A data that could allow insider trading – two had already been breached and who knows how many more? If we were a client of any of the firms listed above, we would be asking some hard questions about possible previous data breaches and data security – and no doubt some of their clients are doing exactly that.

A Class Action Suit Against Law Firms Failing to Report Breaches?

Inflaming the consternation, *Law360* reported on March 31st that privacy class action law firm Edelson PC was planning to file class action legal malpractice litigation against major law firms over the exposure of confidential information. Jay Edelson, the firm's founder, says the firm began investigating a class action against as-of-yet unnamed law firms over client data breaches nearly a year before the article was published.

Edelson said, "We've heard story after story from our friends on the defense side – it's a worst-kept secret that there are data breaches all the time at law firms, and there are a ton of state laws which require notification of data breaches, and the law firms seem to not care about those laws."

Our own spin is slightly different – we think the firms have weighed the risks and determined that the risk of non-compliance with state data breach laws (and why oh why isn't there a federal law?) is small – in Virginia, as an example, your risk is $150,000 per breach – chump change. The greater risk for law firms (we are sure) is the horrifying thought of major clients beating a path to the exit door.

On May 6th, The Global Legal Post revealed that Edelson had already filed a privacy class action suit against a Chicago law firm under seal (because the breach was not then resolved) and is now asking the court to unseal the complaint.

Edelson also said that as his firm plans a class action, he anticipates state attorneys general and even the Federal Trade Commission may start to

investigate law firm cybersecurity reporting practices. Probably true – and that sidebar note no doubt added fuel to the raging fire.

The Panama Papers: The World's Largest Law Firm Data Breach

Enter the jaw-dropping revelations in early April from what has become known as the Panama Papers. The Panamanian law firm that was breached was Mossack Fonseca, which provides services including incorporating companies in offshore jurisdictions such as the British Virgin Islands. It is the fourth largest provider of offshore services. 2.6 terabytes of data – some 11 million files – were exposed, along with the sort of offshore hiding of monies that has become the stuff of legend in the last few decades. The documents span an almost 40-year period from 1977 when the law firm was formed.

An anonymous source passed the data to the German newspaper *Suddeutsche Zeitung*, which has shared them with the International Consortium of Investigative Journalists (ICIJ). The Consortium has assisted in analyzing the files for over a year. The *BBC* says the documents show how the law firm helped clients launder money, dodge sanctions and evade taxes.

Iceland's Prime Minister resigned, the first prominent political fallout from the leaks. But the firm itself is coming under scrutiny, the *BBC* reporting that it worked with 33 individuals or companies who have been placed under sanctions by the U.S. Treasury, in some cases continuing the representation after the sanctions were in place.

Vladimir Putin was apparently involved with $2 billion in offshore accounts. A member of FIFA's Ethics Committee (that has GOT to be a misnomer) was exposed. Others included drug dealers, arms traders, human traffickers and fraudsters.

Round two of the Panama Papers was released in searchable format on May 9th.

While the ICIJ did not include a "data dump" of the original documents or the large-scale release of personal data, it proclaimed the dump likely to be "the largest ever release of secret offshore companies and the people behind them."

You can search the Panama Papers by name or country at https://offshoreleaks.icij.org/ – more than 200,000 entries are included including some of the world's most venerable law firms. Named in the Panama Papers are:

Akin Gump Strauss Hauer & Feld in New York

Arnold & Porter, via legacy firm Howard Rice Nemerovski Canady Falk & Rabkin in San Francisco

Ashurst, via legacy firm Blake Dawson Waldron in London and Sydney

Baker & McKenzie in Bangkok, Hong Kong, Singapore, Stockholm, Taipei and Zurich

Bryan Cave in New York and St. Louis

Coudert Brothers, now defunct, in Denver, Los Angeles, New York and Singapore

Dentons, via legacy firms Denton Wilde Sapte in Gibraltar and Salans Hertzfeld & Heeilbroun in Paris

DLA Piper in Hong Kong and Singapore

Dorsey & Whitney in Hong Kong

Freshfields Bruckhaus Deringer in Singapore

Greenberg Traurig in Miami and New York

Hogan Lovells, via legacy firm Hogan & Hartson in Moscow

Hughes Hubbard & Reed in Miami

Jones Day in Hong Kong and Tokyo

K&L Gates in Hong Kong

Kaye Scholer in Los Angeles

Katten Muchin Rosenman in Chicago

King & Wood Mallesons, via legacy firms Arculli Fong & Ng in Hong Kong and Mallesons Stephen Jaques in Hong Kong

Kramer Levin Naftalis & Frankel in New York

Linklaters in Hong Kong

Morgan, Lewis & Bockius in Singapore

Norton Rose Fulbright, via legacy firms Fulbright & Jaworski in Hong Kong and Macleod Dixon in Calgary

Orrick, Herrington & Sutcliffe in Singapore

Perkins Coie in Taipei

Schiff Hardin in New York

Snell & Wilmer in Costa Mesa, California

Squire Patton Boggs, via legacy firms Deacons Graham & James in Kowloon/Hong Kong and Squire, Sanders & Dempsey in Hong Kong and Los Angeles

Troutman Sanders in Hong Kong

White & Case in Los Angeles and Singapore

Wilmer Cutler Pickering Hale and Dorr, via legacy firm Wilmer, Cutler & Pickering in Washington, D.

The ICIJ noted in a disclaimer that there are "legitimate uses for offshore companies and trusts" and that it does not "intend to suggest or imply that any persons, companies or other entities have broken the law or otherwise acted improperly." We reiterate that disclaimer!

How Did Mossack Fonseca Get Hacked?

While Mossack Fonseca blamed "an e-mail server attack," no one really believed it. It certainly appears that the firm had no intrusion detection or data loss prevention systems in place or it would have known about the breach. If true,

that in itself is a disgrace given their clientele and the kind of work the firm was doing.

As others began to investigate, *The Register* reported that a SQL vulnerability (allowing database commands and values to pass to an application without any validation) was found at the firm. *Naked Security* reported that, aside from the e-mail server hack which the firm acknowledged, the company's WordPress website included a buggy plug-in and that the firm's customer portal was running a long-outdated version of Drupal. Some experts still believe insiders were involved but the firm denies it and we have as yet seen no proof of it.

The New York Times revealed on April 13th that the government had raided the offices of Mossack Fonseca, accompanied by financial analysts and digital forensics experts, looking for evidence of illegal activities, including assisting clients in laundering money and avoiding taxes.

More firms have been named in connection with the Panama Papers, including JP Damiani & Associates (Switzerland), Child & Child (UK), Junod Muhlsteing (Switzerland) and Krinzman Huss (US). This should not be construed as an accusation of illegal activities by those firms. The dust hasn't settled on that either.

The New Yorker observed that other countries tended to use the services of Mossack Fonseca more than U.S. entitles; however, of the fourteen thousand intermediaries—banks, law firms, company-incorporation firms, and other middlemen—with which Mossack Fonseca worked over the years in order to set up companies, foundations, and trusts for its customers, six hundred and seventeen were based in the United States. Most of these are now identifiable from the searchable database.

The FBI Sends Cybersecurity Alerts via the ABA

On April 12th, many ABA members were surprised to find an e-mail from ABA President Paulette Brown in their Inbox. She was advising them that the FBI had requested the ABA to share FBI Private Industry Notification cybersecurity alerts with the legal community. It no doubt startled a lot of lawyers that the FBI was so specifically worried about the vulnerabilities in the legal industry that it would

seek the cooperation of its largest association in getting the word out about threats and defenses.

It has taken law firms a very long time to wake up to the depth and breadth of the threats to their data. The FBI issued its first alert to law firms in 2009, advising them they were being targeted because of the nature of the data they hold on behalf of so many clients and because their security is weaker than that of their clients. A number of such alerts from the FBI have been distributed via the ABA.

More on Law Firm Data Breaches

InfoRisk Today cited yet again on April 7th the reason why law firms are such attractive targets for hackers. Remember the bank robber Willie Sutton? When asked why he robbed banks, he replied, "Because that's where the money is." Likewise, for hackers, law firm networks are where client secrets exist – and that too is where the money is. The post cites the fact that cybersecurity firm Mandiant (now a division of FireEye) estimated that 80 law firms were hacked in 2011 alone.

Bloomberg reported in February of 2016 that Fox Rothchild, Holland & Knight, Hunton & Williams, Simpson, Thacher & Bartlett, Thompson Hine and Wilson Sonsini were all victims of trading schemes that involved employees attempting to compromise and profit from client data. Insiders or outsiders, the myth of law firms carefully guarding client data is vaporizing.

Where Law Firms Should Go From Here

This is going to be a "drip, drip, drip: story as journalists and government authorities seek to connect the dots. As NBC News has already reported, the IRS has warned Americans named in the Panama Papers to come clean before it fully analyzes the Panama Papers. The Treasury Department estimated last year that more than $300 billion dollars of illicit proceeds are generated in the United States annually, with criminals using such companies here and abroad to launder funds. It also intends to issue a long-delayed rule forcing banks to seek the identities of people behind shell-company account holders.

Meanwhile, NBC news reports that federal agents and prosecutors are "chomping at the bit" to exploit the Panama Papers and launch prosecutions according to a senior federal law enforcement official.

You may recall that *60 Minutes* did a segment recently exposing how helpful U.S. lawyers might be in concealing questionable funds. The results were dismal, with only one lawyer flatly refusing to have any part of concealing such funds. Our guess is that the breach of Mossack Fonseca will lead to investigations of involvement in illegal activities by a number of American companies, including law firms. The data leaker here appears to have been a “moral “ leaker who wanted to disclose wrongdoing.

As law firm breaches proliferate, more and more will be known about the unethical or illegal conduct of some lawyers/law firms. State-sponsored hackers from China, Russia, North Korea, etc. may well reveal such information for reasons of their own. For those U.S. firms that may have been involved in questionable activities, it is time to clean house – or to take proactive steps to make sure that the house stays clean. In a breach driven and almost entirely digital world, there really is no place to run and no place to hide if you are caught engaging in unethical or illegal activities.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com