THE PANAMA PAPERS

The 2.6 Terabyte Data Compromise

Abstract

An in-depth discussion of the first data breach of its size in history, exploring the after effects of the breach and how it has impacted law offices around the world.

WhiteHawk Inc.
By Ron White
Case Study
March 2018

THE PANAMA PAPERS: THE 2.6 TERABYTE DATA COMPROMISE

EXECUTIVE SUMMARY

In early 2015, a whistleblowing hacker—angry over massive concealment and growing income inequality around the world—broke into files of the Panamanian law firm Mossack Fonseca. This action resulted in the release of some 11.5 million documents, and at the time, the largest data breach in history. Due to the sheer volume of documents, a historic and continuing cooperative effort involving more than 400 investigative journalists from 100 media organizations across 80 countries was organized to research the files and create searchable online databases. Beginning in April 2016, published articles on the Papers revealed an unseen view into offshore banking and the practices of how the world's wealthy and famous avoid paying taxes and hide potentially illegal or embarrassing financial activities. The breach involved at least 12 current or former world leaders.

Investigators so far have found that the US Treasury Department blacklisted more than 30 of the law firm's clients at one time or another for various financial crimes, which included deals with Mexican drug lords, the terrorist group Hezbollah, and rogue nations such as North Korea and Iran. The data also shows that more than 500 banks and their subsidiaries have driven the creation of at least 15,000 hard-to-trace companies in offshore havens through Mossack Fonseca. A huge surprise for the investigators was that even though Mossack Fonseca created and sold more than 214,000 offshore shell companies, most of the firm's offshore banking clients were within the law.

According to the ABA Journal, the annual cost of Intellectual Property theft in three major categories may be as high as $600 billion, and that the low-end total exceeds $225 billion, or 1.25 percent of the US economy.

Nevertheless, Mossack Fonseca's co-founders are currently fighting money laundering charges and have been detained in Panama since February 2017. In March 2017, the law firm dismissed 250 employees from its offices worldwide because of the "current media, political, and economic environment," according to a statement issued by the company.

THE STORY

In early 2015, an anonymous hacker, angered by extensive banking secrecy and growing income inequality around the world, gained access to the files of Mossack Fonseca, a prominent law firm in Panama, and exposed about 11.5 million documents to the world. At the time, it was the largest single data breach in history and revealed how a global industry of law firms and large banks sell financial secrecy to politicians, billionaires, celebrities, sports stars, and criminals. The data, covering a timeline of more than 40 years, exposed the firm as one of the world's principal creators of shell companies—more than 214,000 and counting—that are linked to more than 200 countries and territories. To date, the data links 140 politicians from more than 50 nations connected to offshore companies in 21 tax havens.

Investigators found Mossack Fonseca's clients on every continent and in a wide range of business activities, including the African diamond trade, the international art market, and other businesses that thrive on secrecy. The firm serviced companies and individuals who sought tax shelters for prominent world leaders and Middle East royalty.

Suddeutsche Zeitung, Germany's largest newspaper and the first media entity contacted by the hacker, and the International Consortium of Investigative Journalists (ICIJ) led a historic and continuing effort to make sense of

the enormous amount of data. They organized a team of more than 400 journalists from 100 media organizations and 80 countries to research the files, prepare them for online access, and publish articles based on their research. The first articles on the Panama Papers appeared in April 2016, and the ICIJ intends to release a full list of companies and people linked to the papers in May 2018.

Among the most prominent and current world leaders already named or otherwise linked to Mossack Fonseca's files include Chinese President Xi Jinping—a hardliner on corruption—and Russian President Vladimir Putin. President Xi's close family members have been linked to embarrassing and potentially corrupt activities tied to offshore accounts. Two of President Putin's sons and other members of his inner circle have been involved in offshore transactions worth more than $2 billion. Mossack Fonseca's records reveal a pattern of covert maneuvers by banks and companies to move transactions as large as $200 million at a time. Putin's sons and associates disguised payments, backdated documents, and gained hidden influence in Russia's media and automotive industries. Although President Putin was not specifically named in the files, these activities could not have occurred without his direct knowledge.

As authorities in Panama gained greater understanding of Mossack Fonseca's offshore banking activities, they arrested the co-founders of the law firm, Jurgen Mossack and Ramon Fonseca, on money laundering charges in February 2017. Mossack Fonseca's defense lawyer argued that the law firm was not at fault in cases where offshore companies it created for clients were later used for illegal activities. As the ICIJ investigation continues and additional files are released to the public, authorities in several countries are conducting investigations of companies and individuals whose offshore banking activities may have been illegal. Meanwhile, the law firm has dismissed 250 employees from branches around the world, and Mossack and Fonseca remain detained.

Additional fallout from the publication of the Panama Papers continues, with international governments conducting investigations on the individuals and banks exposed in the leak of Mossack Fonseca's files. While there is wide agreement on the need for banking reform, world leaders have already faced consequences from the revelations of hidden funds and potential financial crimes. For example, Iceland's Prime Minister resigned when he and his wife were discovered to have secretly owned an offshore firm with millions of dollars in bank bonds during Iceland's financial crisis. And British Prime Minister David Cameron had to explain untaxed profits from an offshore fund set up by his father.

THE LEGAL INDUSTRY

Because law firms conduct investigations of many types for their clients and hav e access to sensitive information and intellectual property by their clients, they will continue to be targets of ever-more sophisticated cyberattacks. The American Bar Association's (ABA's) 2017 Legal Technology Survey Report found that 22 percent of respondents experienced a cyberattack or data breach at some point, an increase of 8 percent over 2016.

The legal industry is facing serious cybersecurity threats from criminals and foreign intelligence organizations. A recent *ABA Journal* article states large firms that rely extensively on international electronic communications may be vulnerable, especially if they operate in countries such as Russia or China where hacking is commonplace. The ABA estimates the annual cost of intellectual property theft in the United States may be as high as $600 billion, or 1.25 percent of the US economy.

22 percent of respondents experienced a cyberattack or data breach at some point in 2017, an increase of 8 percent over 2016.

- American Bar Association

In a data breach even larger than the Panama Papers, the files of the British offshore law firm Appleby were professionally hacked into at some point in 2016, according to a Business Insider report from October 2017. The 13.4 million files, referred to as the Paradise Papers, from this

breach have also been released to the German newspaper, *Suddeutsche Zeitung*. The ICIJ has assembled 95 media partners to examine the documents. The ICIJ intends to publish articles revealing accounts that will name, among others, the Queen of England and Apple.

Because of these cyberattacks, many law firms worldwide are starting to focus more resources on cyber security programs. According to the December 2017 edition of the *ABA Journal*, such a cyber security program should include:

- risk management and incident response planning;
- training for all staff members;
- identification, location, and accessibility of a firm's most valuable data assets;
- a capability for real-time monitoring;
- ensuring that contractors can adequately protect shared data;
- frequent practice on what their response would be if a data breach occurs; and
- establishing a cooperative relationship with law enforcement.

A LUCRATIVE TARGET FOR CYBER CRIMINALS GLOBALLY

Still, the legal industry is facing serious cyber security threats from criminals and foreign intelligence organizations. Hackers are often hired for corporate espionage purposes and by foreign intelligence services seeking to steal everything from intellectual property secrets to government classified information.

Foreign intelligence services use phishing attacks in especially effective and creative ways. Malware hidden in email attachments can quickly infect an entire network and expose sensitive data when users open innocent-looking attachments. Because large law firms often have clients in the defense industrial sector, intelligence services are also seeking sensitive, but unclassified, information on military projects.

In 2016, *Fortune Magazine* said it had seen evidence that people with ties to the Chinese government carried out a 2015 series of attacks on prestigious law firms in the United States. Although a clear motive for the attacks was not disclosed, the attackers appeared to be seeking economic information, possibly for insider trading activities. Insider threat is a valid concern for all industries. In 2016 alone, 69% of enterprise security professionals reported that they had experienced an attempted theft or data corruption practiced by the company's insiders. From a law firm perspective specifically, the 2017 Law Firm Cyber Security Scorecard found that as many as 40% of law firms that were breached from 2016-2017 did not know they were.

Mossack Fonesca was not found to be in violation of specific ABA rules of conduct, which primarily focus on attorney-client privilege. For the most part, ironically the lawyers and clients were working in line with the law. However, from an information assurance and cybersecurity standpoint, it is important to note that the extent of this data breach would have been mitigated had Mossack Fonesca implemented a standard access control protection program (for some initial help, see this article for beginning steps on setting up an access control program) An access control program would have limited online file access, and even if an individual does have access, it would have alerted supervisors to the data flow from their servers. These are very basic and affordable solutions that law firms of all sizes should implement in order to provide the most basic protections to their clients and case data sets, thereby minimizing their online risks.

Globally law firms will continue to be prime targets for cyber criminals, hackers, and foreign governments, and as with physical security, have an obligation to smartly address and mitigate cyber risks. If you have any questions about any part of this article, please visit our website or contact Advisory Services online or at (833) 942-9237 to complete a complimentary Cyber Risk Profile to determine your cyber baseline and basic needs.