ISSN : 1875-4120
Issue : Vol. 16, Issue 3
Published : May 2019

This paper is part of the TDM Special Issue on **"Cybersecurity in International Arbitration"** prepared by:

Stephanie Cohen
Independent Arbitrator
View profile

Mark C. Morril
MorrilADR
View profile

Transnational Dispute Management
www.transnational-dispute-management.com

Cybersecurity Insurance for Law Firms
by P.A. Halprin, G.E. Brown and W. Chiapaikeo

About TDM

TDM (Transnational Dispute Management): Focusing on recent developments in the area of Investment arbitration and Dispute Management, regulation, treaties, judicial and arbitral cases, voluntary guidelines, tax and contracting.

Visit www.transnational-dispute-management.com for full Terms & Conditions and subscription rates.

Open to all to read and to contribute

TDM has become the hub of a global professional and academic network. Therefore we invite all those with an interest in Investment arbitration and Dispute Management to contribute. We are looking mainly for short comments on recent developments of broad interest. We would like where possible for such comments to be backed-up by provision of in-depth notes and articles (which we will be published in our 'knowledge bank') and primary legal and regulatory materials.

If you would like to participate in this global network please contact us at info@transnational-dispute-management.com: we are ready to publish relevant and quality contributions with name, photo, and brief biographical description - but we will also accept anonymous ones where there is a good reason. We do not expect contributors to produce long academic articles (though we publish a select number of academic studies either as an advance version or an TDM-focused republication), but rather concise comments from the author's professional 'workshop'.

TDM is linked to **OGEMID**, the principal internet information & discussion forum in the area of oil, gas, energy, mining, infrastructure and investment disputes founded by Professor Thomas Wälde.

Cybersecurity Insurance for Law Firms

By Peter A. Halprin, Grant Brown, Wendy Chiapaikeo

I. Introduction

As lawyers, it seems like hardly a day goes by without receiving a suspicious email. The emails take many forms but generally seem to entail phony requests from firm management for money, sham new client inquiries, or invitations to download suspicious documents from questionable links. These emails are intended to aid unseen, outside forces in obtaining funds, information, or access. Luckily, at least in the authors' experience, these efforts are generally thwarted.

Unfortunately, they are not always avoided. In February 2014, Thirty Nine Essex Street, a prestigious barristers' chambers in London, was attacked by hackers who compromised the firm's website in an effort to access information about the firm's clients in the energy sector. In July 2015, the website of the Permanent Court of Arbitration was attacked during the pendency of the China-Philippines' boundary dispute arbitration. It was reported that the website was implanted with malicious code that posed a risk to individuals (likely lawyers) who visited a specific page on the website devoted to the boundary dispute.

Attacks on law firms and lawyers are becoming increasingly common as law firms are viewed as "soft targets." In one example, a cybersecurity firm was asked to attack a prestigious law firm's computer systems. According to the CEO of the cybersecurity firm, "in less than 48 hours we had full control of the network, all assets including servers and shares, and all of the users' mailboxes."[1] When asked to probe the computer systems of one of the world's leading technology companies, it took the cybersecurity firm three weeks to access the company's systems and obtain data on mergers and acquisitions. According to the CEO, "we could have gotten that very same data in just a couple of hours if we had targeted the lawyers."[2]

The threats to law firms include the direct theft of funds, data breaches of sensitive client information (including those by so-called hacktivists), malware attacks, phishing attacks, and ransomware attacks. Law firms are also at risk from the inside as disgruntled employees or the inadvertent loss of a computer or blackberry can put sensitive client data at risk. These risks threaten law firms' bottom lines and also expose firms to reputational risks. By way of example, the firm of Mossack Fonseca, which opened in 1977 and was one of the largest firms in the corporate services industry, was forced to shut its doors after a recent devastating data breach that exposed its high-profile clients' secrets to the world.

Given the significant financial exposure, law firms will look to their insurance coverage to help mitigate risk. The good news is that a number of different types of insurance policies may be responsive. Depending on the nature of the risk, policies including those covering

[1] Angie Singer Keating & Jordan M. Rand, *Targeting Law Firms: Cyber Criminals Want What You Got*, THE PHILADELPHIA LAWYER, at *13, Winter 2017, http://www.philadelphiabar.org/WebObjects/PBA.woa/Contents/WebServerResources/CMSResources/TPL_Winter17_cybersecurity.pdf.
[2] *Id.*

crime, cyber, directors and officers, errors and omissions or other professional liability risk, and property damage may be brought to bear.

This article reviews some of the common cyber threats facing law firms, drawing on real-world examples, and then looks to case law on related insurance coverage issues to help law firms assess whether the programs they have in place will respond to the likely threats.

Part II briefly examines threats. As a point of departure, one need look no further than *A Call to Cyberarms*, the article by Stephanie Cohen and Mark Morril, which was the clarion call that gave rise to this special TDM issue. As set forth there:

> Cyberintrusion, or hacking as it is more commonly known, is often in the news in respect to geo-politics and major corporate and government records data breaches. Law firms, too, are increasingly reported as fallen victim to cyberattacks. As awareness increases that corporations and players in the legal sector are attractive targets for cybercriminals, the multiple players involved in international private commercial arbitrations should realize that they too are vulnerable to cybercriminals. International commercial arbitrations routinely involve sensitive commercial and personal information that is not publicly available and that has a potential to move markets or impact competition. Conveniently for hackers, this information is culled together in large data sets, ranging from pleadings and documents produced in disclosure, documentary evidence, witness statements, expert reports, memorials, transcripts, attorney work product, tribunal deliberation materials, and case management data. As the multiple players involved often live in different countries, the information is frequently exchanged and stored in electronic form, making it vulnerable to malevolent outside actors.[3]

Part III focuses on the case law addressing cyber issues in the insurance context—specifically, case law examining coverage for phishing attacks under crime policies; coverage for business interruption following a ransomware attack; and whether professional liability insurance potentially covers the kind of negligence that may enable a phishing attack.

Part IV focuses on potential enforcement liability that may be triggered by hacking attacks that expose confidential information, as occurred with the Panama Papers release, and ensuring policies are responsive to cover ensuing investigations.

II. The Cyber Threat to Law Firms

In today's increasingly digital age, law firms are facing mounting cybersecurity threats. The advent of modern technological developments has brought about significant improvements to the once antiquated legal profession. However, these changes have not been without risks. According to the ABA's 2017 Legal Technology Survey Report, about 22% of participating

[3] Stephanie Cohen & Mark Morril, *A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 Fordham Int'l L.J. 981, 986–87 (2017).

law firms reported that they have experienced some form of a cybersecurity breach.[4] This number represents a significant increase from previous years.[5]

The threat of a cybersecurity breach is a looming risk for all law firms, whether large or small. A testament to the severity of this threat was realized in 2015 and again in 2017 when two global law firms suffered cybersecurity breaches. In 2015, over 11.5 million confidential files from Mossack Fonseca, a Panama law firm with over 500 employees, were leaked by an anonymous source to the International Consortium of Investigative Journalists ("ICIJ").[6] The data breach, known as the "Panama Papers," revealed confidential information pertaining to numerous clients and exposed the firm's involvement in aiding clients evade taxes through offshore accounts.[7] In 2018, the firm announced that it would be shutting down permanently as the result of financial and reputational damage from the leak.[8]

In 2017, DLA Piper, a multinational law firm headquartered in the United Kingdom, fell victim to the NotPetya ransomware attack.[9] As a result of the breach, DLA Piper paid its IT team thousands of hours of overtime to wipe and completely rebuild its internal operating systems.[10] DLA Piper sought coverage for the loss arising out of the NotPetya attack from its insurance company, Hiscox. Hiscox denied coverage and that coverage dispute is presently being arbitrated.[11]

To hackers and cyber-criminals, law firms are attractive "soft targets" for their rich reserves of client data, business secrets, intellectual property, and access to sensitive information regarding mergers and acquisitions and other transactions.[12] Once this information is obtained it can be used as leverage against a firm or sold and traded for profit.[13] In many instances, a successful breach into a law firm's system is a one-stop shop for a wide range of confidential data concerning various clients and matters.

Cybersecurity threats to law firms come in a variety of forms and from a multitude of actors. Some of the more prevalent attacks and data breaches include ransomware, funds transfer fraud, phishing scams, and denial-of-service. The attackers behind these acts include foreign

---

[4] *See* David Ries, *Security*, ABA TECHREPORT 2017, at *2, https://www.americanbar.org/content/dam/aba/publications/techreport/2017/security/security-dave-ries.pdf (last visited Oct. 19, 2018).
[5] *See id.* (stating that 14% of firms experienced a data breach in 2016).
[6] *See* Eric Lipton et al., *Panama Papers Show How Rich United States Clients Hid Millions Abroad*, N.Y. TIMES, Jun. 6, 2016, https://www.nytimes.com/2016/06/06/us/panama-papers.html.
[7] *See id.*
[8] *See Cyber Insurance Market 2018 Q2 Update*, draft, Aon Risk Solutions (Jul. 2018) (on file with author); Nicola Slawson, *Mossack Fonseca Law Firm to Shut Down After Panama Papers Tax Scandal*, THE GUARDIAN, Mar. 14, 2018, https://www.theguardian.com/world/2018/mar/14/mossack-fonseca-shut-down-panama-papers.
[9] Ry Crozier, *DLA Piper paid 15,000 hours of IT overtime after NotPetya attack*, iTnews, May 8, 2018, https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495.
[10] *Id*.
[11] Phil Muncaster, *DLA Piper Set to Sue Insurer Over NotPetya Claim: Report*, Mar. 28, 2019, infosecurity, https://www.infosecurity-magazine.com/news/dla-piper-sue-insurer-notpetya-1-1/.
[12] *See Cyber Insurance Market*, *supra* note 8; Stephanie F. Ward, *Law Firms Can Be Soft Targets for Hackers, Says Cybersecurity Experts*, ABA JOURNAL, Mar. 16, 2017, http://www.abajournal.com/news/article/law_firms_can_be_soft_targets_for_hackers_say_cybersecurity_experts.
[13] *See* Leslie Picker, *3 Men Made Millions by Hacking Merger Lawyers*, *U.S. Says*, N.Y. Times, Dec. 27, 2016 https://www.nytimes.com/2016/12/27/business/dealbook/new-york-hacking-law-firms-insider-trading.html?_r=0.

entities, terrorist organizations, individual sophisticated hackers, nation-states, and a firm's own employees.

Ransomware, a type of "malware" or malicious software, encompasses the vast majority of attacks on law firms and businesses.[14] A common form of the attack is delivered through a link or attachment that appears innocuous but, once clicked, encrypts files and networks, locking out users and, in some cases, threatening to destroy files. A ransom is demanded, usually in the form of money or bitcoin, and until that amount is paid the users are held as hostages. Payment of the ransom does not guarantee that decryption will follow. Furthermore, once breached, a firm's network may be considered compromised.

Another common cybersecurity threat against law firms is funds transfer fraud or "man-in-the-middle attack."[15] This type of attack is accomplished by a third party who sends urgent instructions to a law firm from a legitimate email address purporting to be a current client or another party involved in a transaction with the firm. The instructions direct the firm to transfer funds to a fraudulent account, unbeknownst to the firm.[16] The firm completes the transfer and only learns of the scheme after it is too late to cancel the transfer or recover the funds.

Phishing or spear-phishing in these cases, is defined as "an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer."[17] According to Kaspersky Lab, "[m]any times, government-sponsored hackers or hacktivists are behind these attacks."

A "denial of service" or DOS attack is used to tie up the resources of a website so that users cannot access it.[18] As explained by the Symantec Corporation, this is how such an attack works:

> When the server receives your computer's message, it sends a short one back, saying, in a sense, "Okay, are you real?" Your computer responds – "Yes!" – and communication is established. The website's homepage then pops up on your screen, and you can explore the site. Your computer and the server continue communicating as you click links, place orders, and carry out other business.
>
> In a DOS attack, a computer is rigged to send not just one "introduction" to a server, but hundreds or sometimes thousands. The server—which cannot tell that the "introductions" are fake—sends back its usual response, waiting up to a minute in each case in order to hear a reply. When it gets no reply, the server shuts down the

[14] *See Cyber Insurance Market*, *supra* note 8.
[15] *See id.*
[16] *See* Scott R. Schaffer et al., *Victims of Social Engineering Fraud: A Trend You Do Not Want to Follow*, AON ATTORNEYS ADVANTAGE, https://www.attorneys-advantage.com/Risk-Management/Victims-of-Social-Engineering-Fraud-A-Trend-You-D (last visited Sept. 30, 2018).
[17] *See What is Spear Phishing? – Definition*, KASPERSKY LAB, https://usa.kaspersky.com/resource-center/definitions/spear-phishing (last visited October 21, 2018).
[18] *DOS Attacks Explained*, SYMANTEC, https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html (last visited October 21, 2018).

> connection, and the computer executing the attack repeats, sending a new batch of fake requests.[19]

As technology continues to evolve, so too do the species of malware and the variety of undetectable cyberattacks. The dialogue concerning the potential of a breach has shifted from matters of "ifs" to matters of "when."[20] In light of current trends and past instances, data breaches and cybersecurity threats to law firms are likely to increase. The recognition of this reality is the first step in a law firm's ability to respond to an attack and mitigate any resulting harm in its aftermath.

III. Cyber Insurance Case Law

This Part will discuss cases in which law firms and companies sought to recover under their insurance policies for financial losses caused by cyberattacks in order to determine which policies may be responsive to certain types of cyber threats. Where a case has been adjudicated by a court, this article will examine the court's rationale for holding that a loss caused by a cyberattack was covered by an insurance policy. Subpart A will examine crime insurance coverage and, more specifically, why the trend is that courts have found it responsive in the context of phishing attacks.[21] Subpart B will discuss a recent case in which a law firm sought coverage under a business interruption policy for losses resulting from a ransomware attack.[22] Finally, Subpart C will consider the applicability of professional liability insurance in the cyber context by considering an analogous case.[23]

A. Crime Coverage for Phishing Attacks

Although the authors are unaware of any recent cases examining crime coverage for phishing attacks against law firms, two appellate court decisions rendered in 2018 may be instructive for law firms. In those cases, the United States Court of Appeals for the Second and Sixth Circuits found coverage for policyholders who have suffered losses caused by phishing attacks under the "Computer Fraud" provisions in their crime insurance policies. For good measure, a third case—involving a law firm seeking coverage under a crime policy in 2010—is included in this discussion.[24]

In *Medidata Sols., Inc. v. Fed. Ins. Co.*,[25] Medidata Solutions, Inc. ("Medidata"), a technology company, lost more than $4.7 million after falling victim to a fraudster's phishing scheme.[26] Using a computer code, the fraudster created email messages that appeared to originate with a company executive.[27] The fraudulent emails displayed the executive's full name, email address, and photograph in the "FROM" field of the email message and also

---

[19] *Id.*
[20] Joseph Salvo et al., *Cybersecurity and the Lawyer's Standard of Care*, ABA COMMERCIAL & BUSINESS LITIGATION, May 22, 2018, https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2018/spring2018-cybersecurity-and-the-lawyers-standard-of-care.html.
[21] See *infra* Part III.A.
[22] See *infra* Part III.B.
[23] See *infra* Part III.C.
[24] Per *infra* Part III.B, the decision in that matter was vacated pursuant to the parties' stipulation, presumably following a settlement.
[25] 729 F. App'x 117 (2d Cir. 2018).
[26] *Id.* at 117.
[27] See Brief for Plaintiff-Appellee, Medidata Sols., Inc. v. Fed. Ins. Co., 729 F. App'x 117 (2d Cir. 2018), 2018 WL 1215236, at *9–11.

included his signature at the end.[28] The fraudster used the fraudulent email account to email three employees, requesting that they wire funds to a bank account in order to finalize an acquisition by the company.[29] The employees complied.[30]

After learning that it had been defrauded, Medidata filed a claim with its insurance company, Federal Insurance Company ("Federal"), under the "Crime Coverage Section" of its "Executive Protection" policy.[31] The "Crime Coverage Section" provided coverage for "direct loss[es]" that Medidata sustained as a result of "Computer Fraud," as well as "Funds Transfer Fraud" and "Forgery."[32]

The policy defined "Computer Fraud" as "the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation."[33] "Computer Violation," in turn, was defined as the entry or deletion of "Data" from a Computer System, or a "change to Data elements or program logic of a Computer System."[34] Medidata claimed that coverage was triggered under the "Computer Fraud" provision, amongst other provisions.[35] Federal, however, denied coverage.[36]

Medidata brought suit against Federal for breach of contract, asserting, *inter alia*, that its losses were covered by the "Computer Fraud" provision.[37] Federal argued that it properly denied coverage because (1) the provision only covered "hacking-type intrusions" and (2) Medidata did not sustain a direct loss.[38] The United States District Court for the Southern District of New York disagreed with Federal and awarded Medidata over $5.8 million in damages and interest.[39] Federal appealed and the Second Circuit affirmed.[40]

The Second Circuit explained that the "plain and unambiguous language of the policy covers the losses incurred by Medidata . . . ."[41] First, the court held that a "Computer Violation" occurred when the fraudster manipulated Medidata's email system, which was considered a part of the "Computer System" within the meaning of the policy.[42] It reasoned that the code the fraudster used to alter the appearance of the email messages "represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email

---

[28] *Id.* at *7. In addition, replies to the fraudulent email went to the fraudster rather than the high-ranking member.
[29] *Id.* at *7–8.
[30] *Id.*
[31] *Id.* at *12.
[32] *Id.*
[33] *Id.* at *13.
[34] *Id.* at *14.
[35] *Id.* at *13.
[36] *Id.*
[37] *Medidata*, 729 F. App'x at 118. Medidata also argued that the "Funds Transfer Fraud" and "Forgery" provisions of the insurance policy covered its losses.
[38] *Id.* at 118–19.
[39] *Id*. at 117. The District Court also found coverage under the "Funds Transfer Fraud" coverage, noting that, "[t]he fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny." *Medidata Solutions, Inc. v Fed. Ins. Co.*, 268 F. Supp. 3d 471, 480 (S.D.N.Y. 2017).
[40] *Medidata*, 729 F. App'x at 117.
[41] *Id.* at 118.
[42] *Id.*

system."[43] The court also stated that the phishing attack changed a data element of the computer system because it altered the appearance of email messages.[44] Thus, the court concluded that the cyberattack fell squarely within the terms of the "Computer Fraud" provision.[45]

The court also held that Medidata sustained a direct loss as a result of the phishing attack.[46] It rejected Federal's argument that because Medidata employees were the ones that initiated the transfer, the fraudster did not directly cause the loss.[47] Applying New York law, the court explained that "direct loss" has the same meaning as proximate cause.[48] It concluded, "[w]hile . . . the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the [phishing] attack and the losses incurred. The employees were acting, they believed, at the behest of a high-ranking member of Medidata."[49] Because the court held that the computer fraud provision was applicable, it did not consider whether Medidata's loss was covered by other provisions of the policy, namely the "Funds Transfer Fraud" and "Forgery" provisions.[50]

In *Am. Tooling Ctr., Inc v. Travelers Cas. & Sur. Co. of Am.*,[51] the Sixth Circuit also concluded that a "Computer Fraud" provision was responsive to losses resulting from a phishing attack. In that case, American Tooling Center, Inc. ("ATC"), a Michigan-based tool and die manufacturer, outsourced some of its manufacturing orders to Shanghai YiFeng Automotive Die Manufacture Co., Ltd. ("YiFeng"), a Chinese company.[52] As part of their practice, ATC paid YiFeng in installments based on the amount of work YiFeng completed on a particular order.[53] ATC made its payments via wire transfer using banking software.[54] In March 2015, ATC's Vice President and Treasurer ("ATC's VP") emailed a YiFeng employee requesting that the employee provide him with all outstanding invoices.[55] That email, however, was intercepted by a fraudster "through means unknown[.]"[56] The fraudster, pretending to be the YiFeng employee, corresponded with ATC's VP about the outstanding invoices and eventually asked him to wire payments to a different account because of an audit against YiFeng.[57] ATC's VP did so, and the fraudster repeated the scam twice more.[58] By the time ATC learned of the scam, it had transferred approximately $834,000 to the

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.* at 119.
[47] *Id.*
[48] *Id.* (citing New Hampshire Ins. Co. v. MF Glob., Inc., 108 A.D.3d 463, 970 N.Y.S.2d 16, 19 (1st Dep't 2013)).
[49] *Id.*
[50] Id.
[51] 895 F.3d 455 (6th Cir. 2018).
[52] *Id.* at 457.
[53] *Id.*
[54] *Id.* at 458.
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*

illegitimate banking account.[59] ATC agreed that it would pay YiFeng half of the outstanding debt and that payment of the remaining half would be contingent upon its insurance claim.[60]

During the course of the scam, ATC held a "Wrap+" business insurance policy from Travelers Casualty and Surety Company of America ("Travelers").[61] The policy contained a "Computer Crime" section, which contained the following "Computer Fraud" provision: "The Company [Travelers] will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud."[62] The policy defined "Computer Fraud" as

> The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Financial Institution Premises:
>
> 1. to a person (other than a Messenger) outside the Premises or Financial Institution Premises; or
> 2. to a place outside the Premises or Financial Institution Premises.[63]

ATC filed a claim with Travelers, seeking recovery under the "Computer Fraud" provision, but Travelers denied the claim.[64] ATC then sued Travelers for breach of contract, but the United States District Court for the Eastern District of Michigan granted summary judgment in Travelers' favor.[65] ATC appealed the grant of summary judgment and the Sixth Circuit reversed.[66]

Before the Sixth Circuit, Travelers argued that there was no coverage under the "Computer Fraud" provision because the phishing attack was not "Computer Fraud."[67] Travelers maintained that although there was a fraudulent transfer of funds, the transfer was not caused by a computer, rather the computer was only incidental to the fraud.[68] The Sixth Circuit disagreed.[69] The Court reasoned that the fraudster emailed ATC using a computer and that those emails caused ATC to wire money to the fraudster.[70] The Sixth Circuit found that the policy language was not expressly limited to hackings and that if Travelers wanted the policy to be narrower it could have drafted it as such.[71]

The Sixth Circuit also rejected Travelers' other arguments—that ATC did not suffer a "direct loss" and that ATC's loss was not "directly caused" by "Computer Fraud."[72] Assuming for the sake of argument that "direct" meant "immediate," the court held that ATC sustained a "direct loss" because it "immediately lost its money when it transferred the approximately

---

[59] *Id.* at 457.
[60] *Id.* at 458.
[61] *Id.* at 457.
[62] *Id.* at 459 (emphasis omitted).
[63] *Id.* at 461 (emphasis omitted).
[64] *Id.* at 458.
[65] *Id.*
[66] *Id.* at 459.
[67] *Id.* at 461
[68] *Id.*
[69] *Id.*
[70] *Id.* at 461–62.
[71] *Id.* at 462.
[72] *Id.* at 459 & 462.

$834,000 to the [fraudster], there was no intervening event."[73] It found meritless Travelers argument that because ATC already owed that money to YiFeng, the loss only occurred when it uncovered the fraud.[74] The court also held that ATC's loss was "directly caused" by the computer fraud because ATC's VP, after being "induced by the fraudulent email," performed internal actions leading to the transfer of funds to the fraudster.[75]

Finally, the Sixth Circuit considered three exclusions that Travelers argued precluded coverage and decided that were inapplicable.[76] The three exclusions were:

- Exclusion R: No coverage for "loss resulting directly or indirectly from the giving or surrendering of Money, Securities or Other Property in any exchange or purchase, whether or not fraudulent, with any other party not in collusion with an Employee."[77]
- Exclusion G: No coverage for "loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System."[78]
- Exclusion H: No coverage for "loss resulting directly or indirectly from forged, altered or fraudulent documents or written instruments used as a source documentation in the preparation of Electronic Data . . . ."[79]

The Sixth Circuit determined Exclusion R was inapplicable because ATC did not transfer the money to the fraudster in exchange for anything from the fraudster.[80] Next, the court held that Exclusion G did not apply because the term "Electronic Data" was defined by the policy and expressly excluded "instructions or directions to a Computer System."[81] Thus, under the terms of the policy, ATC's VP did not input "Electronic Data" when he used banking software to wire funds to the fraudster.[82] The Court noted that Travelers chose to define "Electronic Data" narrowly.[83] Lastly, the Sixth Circuit ruled that Exclusion H was similarly inapplicable as ATC's VP's entries did "not constitute 'Electronic Data' as defined by the Policy."[84]

In *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*,[85] a Connecticut trial court also found that losses resulting from fraud perpetrated through email were covered under a "computer fraud" provision in a crime insurance policy.[86] There, Owens, Schine, & Nicola, P.C. ("OSN"), a law firm, received an email from a person claiming to be an attorney from North Carolina, requesting assistance with a matter for a Chinese client.[87] OSN then

[73] *Id.* at 460.
[74] *Id.* at 459–60.
[75] *Id.* at 463.
[76] *Id.*
[77] *Id.* (emphasis omitted).
[78] *Id.* at 464 (emphasis omitted).
[79] *Id.* at 465 (emphasis omitted).
[80] *Id*. at 463.
[81] *Id.* at 464.
[82] *Id*.
[83] *Id.* at 464–65.
[84] *Id.* at 465.
[85] No. CV095024601, 2010 Conn. Super. LEXIS 2386 (Conn. Super. Ct. Sept. 17, 2010).
[86] The judgment was later overturned based on a stipulation by the parties. *See Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, No. FBT-CV-5024601-S, 2012 Conn. Super. LEXIS 5053, at *1 (Conn. Super. Ct. Apr. 18, 2012).
[87] *See Owens, Schine*, 2010 Conn. Super. LEXIS 2386, at *2.

received an email from a fraudster claiming to be the Chinese client.[88] The fraudster entered into an agreement with OSN whereby the firm would a collect a debt owed to him by a business in Connecticut.[89] The alleged debtor sent OSN a check in the amount of $198,610, which OSN deposited into its trust account.[90] Before the check cleared, OSN, at the fraudster's direction, wired the funds minus the attorney fees to a banking institution in South Korea.[91] All of OSN's correspondence with the fraudster had been through email.[92]

After wiring the money out of its trust account, OSN learned that the check it tried to deposit was fraudulent.[93] OSN filed a claim with its insurance company Travelers, seeking indemnification under the "computer fraud" provision in the Travelers' policy.[94] The computer fraud provision stated, "[w]e will pay you for your direct loss of, or your direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud."[95] The policy defined "Computer Fraud" as "The use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises: [1.] to a person (other than a Messenger) outside the Premises or Banking Premises; or [2.] to a place outside the Premises or Banking Premises."[96]

After Travelers denied its claim, OSN filed suit in the Connecticut Superior Court.[97] Travelers moved for summary judgment, arguing that: (1) OSN's loss was not covered by the policy because the fraudster's action did not constitute computer fraud; (2) an exclusion applied for losses associated with accepting money orders or counterfeit money; and (3) an exclusion applied for surrendering money in an exchange or purchase.[98]

The Court denied Travelers's motion.[99] First, in assessing Travelers's argument that there was no computer fraud because a computer was not used to generate a transfer of funds, the Court held that the term "computer fraud" was ambiguous.[100] The Court reasoned that it was unclear to what extent a computer needed to be used to constitute computer fraud under the policy.[101] Because the policy was ambiguous, the court resolved the ambiguity in favor of OSN, as the policyholder, and opined that any computer usage would suffice to trigger coverage under the computer fraud provision.[102] The Connecticut Superior Court therefore held that since the fraudster used a computer to perpetrate the fraud by emailing OSN, the computer fraud provision was applicable.[103]

---

[88] *Id.*
[89] *Id.*
[90] *Id.* at *3.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.* at *9.
[96] *Id.* at *9–10.
[97] *Id.* at *5.
[98] *Id.* at *5–6.
[99] *Id.* at *33.
[100] *Id.* at *19.
[101] *Id.*
[102] *Id.*
[103] *Id.* Similar to the Second and Sixth Circuits in *Medidata* and *American Tooling*, respectively, the *Owens, Schine* Court held that the computer fraud caused OSN's loss. It likened the term "direct cause" to "proximate cause," which, under Connecticut law, is defined as "the procuring, efficient, and predominant cause." *Id.* at *21

The Court then rejected both the "Counterfeit Money" and "Exchange or Purchase" exclusions.[104] With regard to the former, the policy defined "Counterfeit Money" as "an imitation of money that is intended to deceive and to be taken as genuine."[105] Money was defined as a "medium of exchange in current use and authorized or adopted by a domestic or foreign government, including currency, coins, bank notes, bullion, travelers checks, registered checks and money order held for sale to the public."[106] The Court opined that the bank check that OSN received from the fraudster did not fall into the policy-provided or ordinary definition of "Counterfeit Money," and thus the exclusion did not preclude coverage.[107]

As with the computer fraud coverage, the Court held that the "Exchange or Purchase" exclusion could be interpreted in multiple ways.[108] As Travelers argued, the firm submitted the check in exchange for fees.[109] But as OSN maintained, it did not exchange funds for a fee, rather the money it took from the check was meant to be a retainer for fees that it would negotiate in the future.[110] Because the provision was open to multiple interpretations, the Court construed the policy against Travelers, the insurer.[111]

The foregoing case law demonstrates that crime insurance coverage may be available to law firms seeking to recover in the aftermath of a phishing attack. Policyholders should be aware, however, that the insurance industry may invoke cases from jurisdictions other than the Second and Sixth Circuits that did not find coverage.[112] As such, policyholders should be prepared as they may face opposition to the payment of claims under such policies.

B. Coverage for the Business Interruption Losses Associated with a Ransomware Attack

As noted above, a ransomware attack involves locking companies out of access to their data until a ransom is paid.[113] But, as was also noted in the Aon Report, payment of the ransom does not guarantee that decryption will follow and, once breached, a firm's network may remain compromised.[114] In the case that follows, the ransom was paid, but the financial consequences of the lack of access to data remained with the law firm even after the payment. Seeking to be made whole after its resulting business interruption losses, the policyholder law firm sought coverage under a business owners' insurance policy.

(citation omitted). It reasoned that while the emails by the fraudster did not immediately cause the loss, it nevertheless procured the loss. *Id*. at *23.

[104] *Id.*

[105] *Id.*

[106] *Id.*

[107] *Id.* at *25.

[108] *Id.* at *26.

[109] *Id.*

[110] *Id.*

[111] *Id*. (citing Harrah's Entm't, Inc. v. ACE Am. Ins. Co., 100 F. App'x 387, 391 (6th Cir. 2004)) (considering an identical insurance provision).

[112] *See*, *e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016) (holding that there was no coverage under a crime policy because the email that caused the loss was "merely incidental" to the loss and did not directly cause the loss); Interactive Comms. Int'l Inc. v. Great Am. Ins. Co., 723 Fed. App'x 929 (11th Cir. 2018) (holding that there was no coverage under a "Computer Fraud" policy because policyholder's loss did not "result[] directly" from the fraud).

[113] *See Cyber Insurance Market*, *supra* note 8.

[114] *See id.*

The law firm in question, Moses Afonso Ryan Ltd. ("MAR"), a Rhode Island-based law firm, was the victim of a ransomware attack.[115] An attorney at the firm received an email with an attachment, which he opened.[116] The attachment contained a ransomware virus, which infected MAR's computer network, encrypting all of the firm's computer systems and information so that they were inaccessible.[117] MAR searched for the perpetrators and negotiated multiple ransoms to regain access to their computer system.[118] After MAR paid the perpetrators over $25,000 in cryptocurrency, the perpetrators provided MAR with a decryption tool to recover the firm's documents and information.[119] By the time MAR retrieved the information, however, the firm had lost over $700,000 because they were unable to work productively for three months.[120]

MAR held a business owners' insurance policy with Sentinel Insurance Company Ltd. ("Sentinel") that was in effect during the time the firm was locked-down by the ransomware.[121] The policy insured MAR for "up to 12 months of 'actual loss of Business Income'" that MAR sustained "due to the necessary suspension of [its] 'operations' . . . due to 'physical loss of or physical damage to property.'"[122] The policy also contained a provision for "Computers and Media" coverage, which provided that Sentinel covered MAR for any loss related to "the cost to research, replace or restore physically lost or physically damaged 'data' and 'software'" for up to $20,000.[123]

MAR presented a claim for over $700,000 to Sentinel relating to the business interruption and computer losses caused by the ransomware attack.[124] Sentinel, however, only paid MAR $20,000 for losses under the "Computers and Media" provision. It denied coverage for business interruption.[125] MAR sued Sentinel in the Providence County Superior Court in Rhode Island, arguing that it was entitled to coverage for its business interruption losses.[126] Sentinel removed the case to the United States District Court for the District of Rhode Island.[127]

MAR thereafter moved for partial summary judgment on the issue of whether coverage existed.[128] It asserted that "the necessary suspension of [its] operations was clearly due to physical loss and damage to [its] property (*e.g.,.* its computers, computer system, data, and information) from the cyberattack."[129] The firm argued that property was not defined to include only "tangible" property, and therefore included its intangible property, such as its computer system, data, and information.[130] MAR asserted that there was physical loss of

---

[115] Complaint, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co. Ltd., Case No. 1:17-001570-WES-LDA (Apr. 4, 2017).
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] Plaintiff's Memo. in Support of Mot. for Partial Summary Judgment, Moses Afonso Ryan Ltd. v. Sentinel Ins. Co. Ltd., Case No. 1:17-001570-WES-LDA, at *3 (Dec. 22, 2017).
[123] *Id.*
[124] *Id.* at *4.
[125] *Id.* at *5.
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.* at *9.
[130] *Id.*

property because while the data was encrypted, its employees were physically unable to access it.[131]

The case appears to have settled before the Court had an opportunity to rule on the MAR's motion. Pursuant to a stipulation entered into by the parties, the case was dismissed with prejudice. The case nevertheless demonstrates that business interruption policies, particularly those that are not limited to interruptions stemming from physical damage to physical property, may be responsive in the cyber context.[132] As with the crime coverage referenced in Subpart A, these cases demonstrate that policyholder law firms should look to all potentially responsive policies in the aftermath of a cyberattack.

C. Professional Liability Insurance May Also Be Responsive to Losses Resulting from Cyberattacks

The next case involves old-fashioned fraud against a law firm in relation to a client inquiry and settlement, not involving electronic means. The facts, however, are very close to those now involving electronic means. And, indeed, the client inquiry here is similar those sometimes received by the authors. Although the terms of a particular professional liability policy may limit the ability to recover in the cyber context, the below demonstrates that law firm policyholders should check their policies as they could prove useful in such situations.

In *Nardella Chong, P.A. v. Medmarc Cas. Ins. Co.*, the law firm of Nardella Chong, P.A. ("Chong") was the victim of fraud similar to the fraud perpetrated on OSN.[133] A fraudster, purporting to be a client, contacted Chong, requesting its assistance in forming a subsidiary.[134] The fraudster gave Chong a check and directed it to wire transfer the value of the check, less Chong's legal fees, to an alleged overseas business partner.[135] Chong deposited the check into its clients' trust fund and transferred the funds out of that account before the check cleared.[136] The check turned out to be fraudulent and, thus, Chong had actually distributed funds belonging to its other clients.[137] Chong did not recover the money.[138]

At the time the fraud was perpetrated, Chong owned a professional liability insurance policy from Medmarc Casualty Insurance Company ("Medmarc").[139] The policy covered "all claims of negligence arising from an act or omission in the performance of 'professional services' rendered by" Chong.[140] Professional services were defined to include "services as a . . .

---

[131] *Id.* at *10.
[132] Policyholders should be aware of a recent Illinois state court case involving the insurance company's invocation of a "war exclusion" in light of the NotPeyta malware attack. Complaint, Mondelez Int'l Inc. v. Zurich Am. Ins. Co., Case No. 2018-L-110008 (Oct. 10, 2018).
[133] 642 F.3d 941 (11th Cir. 2011).
[134] *Chong*, 642, F.3d at 942.
[135] *Id.* at 942.
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*

trustee . . . but only for those services typically and customarily performed by an attorney."[141] Chong filed a claim with Medmarc which the insurance company denied.[142]

Chong thereafter sued Medmarc, but the United States District Court for the Middle District of Florida found that there was no coverage, reasoning that Chong did not perform a negligent act in the performance of a professional service.[143]

The United States Court of Appeals for the Eleventh Circuit reversed and held that Chong's claim was covered.[144] The Eleventh Circuit explained that a fiduciary relationship is created when an attorney holds a client's funds and that management of those funds in a trust account constituted a professional service under the terms of the policy.[145] The Eleventh Circuit, therefore, concluded that Chong's erroneous transfer of client's funds was a professional service and, moreover, that it could form the basis of a negligence claim thereby triggering coverage under the policy.[146]

Although *Chong* did not involve a cyberattack, it demonstrates that when a cyberattack (such as a phishing attack) influences an attorney to transfer client funds negligently, a law firm policyholder should consider whether there may be coverage under a professional liability policy.

IV. Mossack Fonseca and Coverage for Subpoenas

Parts II & III illustrates that cyber risks come in many forms and that there are a number of different policies that could assist law firms seeking to be made whole in the aftermath of a cyberattack. This Part discusses a further risk to law firms that suffer following data breaches—regulatory costs—and the coverage that may be available under such circumstances. To facilitate the discussion, we briefly review the Panama Papers.

In April 2016, the ICIJ began reporting on their review of over 11.5 million documents, the private client files of a Panamanian law firm that specialized in trust services, covering a 40-year span.[147] Among other things, documents from the Panama Papers revealed:

- Offshore holdings of 140 politicians and public officials from around the world, including the (now former) prime minister of Iceland, the president of Ukraine, and the king of Saudi Arabia
- More than 214,000 offshore entities connected to people in more than 200 countries and territories
- Major banks' central role in the creation of hard-to-trace companies in offshore havens

---

[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.* at 943. The court also pointed to the Florida Bar Rules of Attorney Conduct, which indicated that management of client funds is a professional service. *Id.*
[146] *Id.*
[147] Bastian Obermayer et al., The Panama Papers - Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption, Int'l Consortium of Investigative Journalists, Apr. 3, 2016, https://panamapapers.icij.org/20160403-panama-papers-global-overview.html.

The outrage generated by the release of the Panama Papers caught the attention of regulators. On April 20, 2016, Preet Bharara, then-United States Attorney for the Southern District of New York, wrote to the ICIJ to seek assistance, as his office was investigating "matters to which the Panama Papers are relevant."[148] In addition, regulators launched investigations in Britain, France, Australia, New Zealand, Austria, Sweden, and the Netherlands.[149]

This regulatory scrutiny should bring into focus some important risks for law firms. Regulators pursuing law firms following data breaches, in addition to requiring compliance with notification and reporting requirements, may investigate law firms liable for aiding and abetting nefarious activity if reports of such activity are brought to their attention.

As noted above, professional liability policies generally protect law firms against loss resulting from acts, errors or omissions in their performance of professional duties. Importantly here, these policies may provide coverage for regulatory investigations.

Law firm policyholders should carefully review the timing and trigger of coverage under such policies. Critically, the amount of coverage available to a law firm in the face of a government investigation may depend on the breadth of the definition of the term "claim" in a given policy.

Although the authors are not yet aware of cases arising in the cyber context, in other contexts courts have found coverage for subpoenas.[150] Indeed, courts throughout the country have found coverage for subpoenas and oral requests for documents.[151]

In addition, to the extent a law firm is incurring costs in conjunction with a regulatory action while at the same time defending civil or arbitration proceedings, and the insurance company is challenging coverage for costs arising out of the subpoena, the costs of investigation may be reasonably related to the defense of those parallel proceedings and could therefore be covered.

The protection afforded by policies that provide coverage for regulatory investigations is exceedingly valuable to any law firm. Negotiating and working with government regulators when investigations are in their infancy is critical to an early and less public resolution of any changes. It can also be expensive. While the associated defense costs may be significant, the facts developed in responding to such an investigation are commonly used to convince the government that formal charges are not appropriate. Accordingly, coverage for defense costs

---

[148] Matt Zapotosky, *U.S. Launches 'Criminal Investigation' Involving Panama Papers*, WASHINGTON POST, Apr. 20, 2016, https://www.washingtonpost.com/world/national-security/us-launches-criminal-investigation-involving-panama-papers/2016/04/20/1358099e-0721-11e6-b283-e79d81c63c1b_story.html?utm_term=.1f6f24aee12d

[149] Kylie MacLellan & Ragnhildur Sigurdardottir, *Iceland's Leader Resigns, First Casualty of Panama Papers*, REUTERS, Apr. 5, 2016, https://www.reuters.com/article/panama-tax/icelands-leader-resigns-first-casualty-of-panama-papers-idINKCN0X225C.

[150] *See* MBIA, Inc. v. Fed. Ins. Co., 652 F.3d 152 (2d Cir. 2011).

[151] *See*, *e.g.*, Polychron v. Crum & Forster Ins. Cos., 916 F.2d 461 (8th Cir. 1990); ACE Am. Ins. Co. v. Ascend One Corp., 570 F.Supp.2d 789 (D.Md. 2008); Minuteman Int'l, Inc. v. Great Am. Ins. Co., No. 03C6067, 2004 WL 603482 (N.D. Ill. Mar. 22, 2004); Syracuse Univ. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, 2012EF63, 2013 N.Y. Misc. LEXIS 2753, at *10 (Sup. Ct. Onondaga Cty. Mar. 7, 2013) ("We reject the insurers' crabbed view of the nature of a subpoena as a 'mere discovery device' that is not even 'similar' to an investigative order."), *aff'd*, 112 A.D.3d 1379 (4th Dep't 2013).

at an informal stage will not only reduce the direct costs but will also be critical in heading off a formal investigation and perhaps even significant fines.

V. Conclusion

The foregoing should give some sense of the scope of risk law firms face today on the cyber front, as well as the potential for obtaining insurance coverage for such risks under common forms of business insurance. Also clear, however, are the potential pitfalls in coverage as currently written and interpreted by insurance companies—including the "direct loss" defense invoked in crime policies, as well as the ambiguities in the terms of coverage for investigations and enforcement actions. Awareness of these pitfalls should inform a firm's purchase and analysis of coverage—just as awareness of the risks of phishing, ransomware, and data-hacking attacks should help companies avoid those risks.

Law firms should work closely with their internal and external finance, insurance, information technology, and operations professionals to help procure insurance to protect them in the event of a cyber incident.