PLI Current

The Journal of PLI Press

Vol. 4, No. 3, 2020

Cyber Insurance: What Case Law Teaches Us About Coverage

Tab R. Turano

Miller Friel, PLLC

I. Introduction

Cybercrime has come a long way from the days of Nigerian Princes seeking aid from unsuspecting AOL subscribers to liberate their family fortunes from the grips of oppressive regimes. Cybercriminals today are far more sophisticated, and so too are their victims. Now, it is C-Suite executives and publicly traded corporations being swindled by ever-evolving "spoofing" scams, while some of the world's largest healthcare providers, airlines and hotel companies fall victim to massive data breaches as a result of "phishing" schemes and other malware. Indeed, recently a handful of multi-national conglomerates had their operations virtually shut down by malware

purportedly released by the Russian military.[1] The costs to companies associated with these modern-day cyberthreats can be staggering. Cybercrime is among the most significant risks facing businesses today. Fortunately, in the event of an attack, companies may not have to go it alone. In many instances, insurance may be available to cover some or all of the loss.

This article highlights a few of the more recent massive cyber incidents inflicted on well-known U.S. companies, and discusses the various types of insurance products marketed and sold to protect businesses against such risks, as well as notable court decisions addressing the scope of cyber coverage under such policies. Finally, some practical pointers are offered for effectively insuring against the risks of modern cyberthreats.

II. The Growing Threat of Cybercrime

Earlier this year, Equifax, the multinational consumer credit reporting agency, finalized the largest data breach class-action settlement in history. The case arose from an incident in 2017 in which hackers accessed personal data, including names, dates of birth, social security numbers and driver's license numbers from approximately 150 million consumers. Ensuing claims were brought by the Federal Trade Commission, the Consumer Financial Protection Bureau and various state attorneys general. More than 300 class-action lawsuits were also filed by consumers and financial institutions, which were consolidated in Federal District Court in Atlanta, Georgia.[2]

The Equifax litigation was ultimately resolved through a settlement agreement executed in September 2019 and approved by the court in January 2020.[3] The agreement, as approved by the court, obligates Equifax to pay a minimum of $380.5 million into a settlement fund for class benefits, attorneys' fees and other ancillary costs

---

[1] Ellen Nakashima, *Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, WASH. POST (Jan. 12, 2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[2] *In re* Equifax Inc. Customer Data Security Breach Litigation, No. 1:17-md-02800-TWT (N.D. Ga.).

[3] *Id.*, Doc. 956.

and expenses.[4] Equifax agreed to pay up to an additional $125 million, if needed, to satisfy additional out-of-pocket losses and potentially $2 billion for class member creditor monitoring. Finally, the settlement requires Equifax to spend at least $1 billion for data security and related technology to prevent future breaches.[5] In sum, the minimum cost to Equifax of the settlement is $1.38 billion, and potentially much more.

The Equifax data breach is far from an isolated incident. Companies of all sizes and industries are hit regularly. Data breach liabilities, which often include costs of notifying customers of the breach, credit monitoring for customers, data recovery costs, public relations or crisis management costs, and, of course, third-party lawsuits and governmental enforcement actions, have spanned from tens to hundreds of millions of dollars. In 2011, for example, hackers infiltrated Sony PlayStation, taking personal and credit card information from over 100 million people and costing Sony an estimated $170 million.[6] Several years later, hackers infiltrated credit card readers at Target locations, walking away with 40 million credit and debit card numbers, leading to an $18.5 million settlement with state attorneys general.[7] In 2015, cybercriminals hit Anthem Inc., one of the country's largest health insurers, stealing names, dates of birth, social security numbers, employment information and income data from tens of millions of Americans.[8] Anthem's deal to resolve the ensuing litigation cost the company an estimated $115 million towards creating a pool to provide credit protection and reimbursement of customer costs. And in 2018, ride-share giant Uber

---

[4] *Id.*, p. 5.

[5] *Id.*, pp. 5, 7.

[6] Jason Schreier, *Sony Estimates $171 Million Loss from PSN Hack*, WIRED (May 23, 2011), https://wired.com/2011/05/sony-psn-hack-losses.

[7] Samantha Masunaga, *Target Will Pay $18.5 Million in Settlement with States over 2013 Data Breach*, L.A. TIMES (May 23, 2017), https://latimes.com/business/la-fi-target-credit-settlement-20170523-story.html.

[8] Fred Donovan, *Judge Gives Final OK to $115M Anthem Data Breach Settlement*, Health IT Security (Aug. 20, 2018), https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement.

agreed to pay $148 million to settle with state attorneys general for failing to disclose a massive data breach that occurred several years prior.[9]

Unfortunately, data breach is not the only cyberthreat companies face. Spoofing[10] and phishing[11] scams are routine, causing employees to unwittingly disclose confidential financial information or to voluntarily transfer millions of dollars to cyberthieves. Malware[12] is capable of causing massive property damage and has even shut down entire business operations at multinational corporations. Take, for example, the recent "NotPetya" malware—a malicious code that, according to U.S. cybersecurity experts, was launched by Russian military hackers and intended to cripple Ukraine's financial system.[13] The malware, which irreversibly encrypted computers' master boot records, quickly escaped its intended targets in the Ukraine and spread across continents, crippling mega-corporations like shipping conglomerate A.P. Moller-Maersk, pharmaceutical giant Merck, and food manufacturer Mondelez International. According to Mondelez, the malicious malware attack "propagated across [its] network, and rendered permanently dysfunctional approximately 1700 of

---

[9] Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html.

[10] "Spoofing," as defined by one court, is "the practice of disguising a commercial e-mail to make the e-mail appear to come from an address from which it actually did not originate," and "involves placing in the 'From' or 'Reply-to' lines…an e-mail address other than the actual sender's address…" Medidata Solutions, Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 477 n.2 (S.D.N.Y. 2017) (quoting Karvaly v. Ebay, Inc., 245 F.R.D. 71, 91 n. 34 (E.D.N.Y. 2007)).

[11] "Phishing" is "a scam by which an internet user is duped (as by deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly." "Phishing." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/phishing (last visited June 13, 2020).

[12] "Malware" is a generic term for software intended to interfere with a computer's normal function, often used to commit cybercrimes by gaining unauthorized access to a computer system. "Malware." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://merriam-webster.com/dictionary/malware (last visited June 5, 2020).

[13] Nakashima, *supra* note 1.

[its] servers and 24,000 of its laptops."[14] Mondelez "incurred property damage, commercial supply and distribution disruptions, unfilled customer orders, reduced margins, and other covered losses" in excess of a billion dollars.[15] Merck likewise alleged that the attack caused extensive disruption to its worldwide operations, including manufacturing, research and sales operations, and caused massive financial losses.[16] All told, NotPetya caused an estimated $10 billion in damage worldwide.[17]

Fortunately, insurance coverage may be available to protect against these types of risks.

III. Insurance Coverage for Cyberattacks

Insurance coverage for data breaches and various other cybercrimes may be found under an array of insurance products, from traditional general liability policies, to crime (or fidelity) policies, to stand-alone cyber insurance policies or endorsements. As cyberthreats continue to evolve, so too do the insurance policies and forms designed to cover such risks. All this, not surprisingly, has led to a surge in insurance coverage litigation and court decisions addressing the nature and scope of insurance coverage for cyber losses. Below, the various types of insurance coverages applicable to cyberthreats, as well as leading judicial opinions addressing coverage under such policies, are discussed.

A. Cyber Coverage Under Traditional General Liability Policies

Historically, companies looked to traditional general liability policies for protection against cyberthreats. Potential coverage for cyber losses may be found under two separate insuring agreements contained in general liability policies: (i) property damage liability; and (ii) personal and advertising injury. The former typically affords

---

[14] *See* Mondelez Int'l., Inc. v. Zurich Am. Ins. Co., Case No. 2018L011008 (Ill. Cir. Ct. Oct. 10, 2018).

[15] *Id.*

[16] Merck & Co., Inc., et al. v. Ace Am. Ins. Co., et al., Case No. UNN-L-002682-18 (N.J. Super. Ct.).

[17] Andy Greenberg, *The Untold Story of NetPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

coverage for amounts a company is "legally obligated to pay as damages" because of "property damage," which is defined to include physical injury to tangible property and any resulting loss of use, as well as the loss of use of tangible property that is not physically injured.[18] Personal and advertising injury coverage, in turn, protects against damages arising from certain enumerated offenses, including "oral or written publication…of material that violates a person's right of privacy.[19] Both of these coverages have given rise to unique legal issues.

i. Property Damage Coverage

The textbook example of cyber-related property damage is a virus that causes a computer system to become non-functional or to operate slower or otherwise less than optimally. Coverage disputes over property damage for cyberthreats typically involve whether or not the insured has suffered physical injury or loss of use of tangible property. The Eighth Circuit's decision in *Eyeblaster Inc. v. Federal Insurance Company* is perhaps the leading case in favor of coverage.[20] There, a computer user sued Eyeblaster, alleging that Eyeblaster damaged his computer after he visited its website. According to the plaintiff, Eyeblaster infected his computer with spyware, which caused his computer to freeze up and crash, caused numerous pop-up ads and random error messages, and slowed performance.[21] The plaintiff claimed he lost data on his tax returns and incurred costs to repair his computer system. Notably, the insurance policy at issue, like many general liability policies, provided that "software, data or other information that is in electronic form" is not "tangible property."[22] Accordingly, Federal argued that the plaintiff did not allege damage to tangible property (which would be covered), but rather sought to recover loss due to damage to software, which was excluded.[23] Eyeblaster asserted to the contrary that the plaintiff alleged the loss of

---

[18] Insurance Services Office (ISO), Commercial General Liability Coverage Form, No. CG 00 01 04 13 (2012), https://www.northstarmutual.com/UserFiles/Documents/forms/policyforms/Current/CG%2000%2001%2004%2013.pdf.

[19] *Id.*

[20] Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (8th Cir. 2010).

[21] *Id.* at 800.

[22] *Id.* at 802.

[23] *Id.* at 801.

use of his computer.[24] The court agreed with Eyeblaster, holding that tangible property, while not defined by the policy, clearly included the plaintiff's computer, and that the plaintiff's complaint "alleges repeatedly the 'loss of use' of his computer," which falls squarely within the general liability policy's definition of property damage.[25]

Notably, a different result was recently reached in *Ciber, Inc. v. Federal Insurance Company*.[26] There, Ciber had entered a contract with the Hawaii Department of Transportation (HDOT) to replace its financial management computer system. The HDOT alleged that the software system Ciber designed failed to perform in that it could not save data and brought the HDOT's computers to a standstill with flashing error messages. Ciber argued that, similar to *Eyeblaster*, the HDOT's allegations alleged loss of use of the HDOT's computer systems. The court, however, found *Eyeblaster* distinguishable. There, according to the court, the plaintiff had lost the use of his computer system because it no longer functioned after installation of new software. Here, in contrast, the HDOT's "theory of recovery [was] based on plaintiff's new software inadequacies, not on losing the use of tangible computer systems."[27] Coverage, therefore, was denied in *Ciber*.

At first glance, *Eyeblaster* and *Ciber* appear difficult to reconcile. But upon closer inspection, the key distinction is likely that in *Eyeblaster*, the plaintiff alleged that the insured installed unwanted spyware on his computer which impacted functionality, whereas in *Ciber*, the underlying claim alleged defects in the design of the insured's product itself. This distinction emphasizes that property damage coverage for cyber claims may be highly fact-dependent.

ii. Personal and Advertising Injury Coverage

General liability policies may also provide coverage for data breaches. Such coverage is potentially found under the personal and advertising injury coverage grant

---

[24] *Id.* at 801–02.

[25] *Id.* at 802; *see also* Retail Systems, Inc. v. CNA Ins. Companies, 469 N.W. 2d 735 (Minn. App. 1991) (holding that computer tape and associated data were tangible property within meaning of general liability property coverage).

[26] Ciber, Inc. v. Federal Insurance Company, Case No. 16-cv-01957-PAB-MEH, 2018 WL 1203157 (D. Colo. Mar. 3, 2018).

[27] *Id.* at *3.

(i.e., publication of personal data as a privacy violation). Here too, there has been substantial litigation throughout the years over whether third-party data breach lawsuits fall within the scope of general liability coverage. Such litigation typically focuses on whether the loss results from "publication," and, if so, who must be responsible for such publication.

In *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC*,[28] the court found coverage for data breach loss. Portal Healthcare specialized in the electronic safekeeping of medical records for various hospitals and clinics. The company was sued in 2013 in a class action alleging that its negligence resulted in patients' medical records becoming publicly accessible over the internet and viewable by unauthorized individuals. Portal Healthcare's insurer refused to defend the company against the class action, contending that the company had not "published" private information. But the court disagreed. Noting that the term "publication" was not defined in the insurance policy, the court ruled that making confidential medical records publicly accessible over the internet falls within the plain and ordinary meaning of the term "publication," and ordered the insurer to reimburse Portal Healthcare for its costs of defense.

More recently, however, two decisions from the District Court for the Middle District of Florida reached a contrary conclusion, denying insureds' demands for defense costs coverage in connection with data breach actions. In *Innovak International, Inc. v. Hanover Insurance Company*,[29] the insured's database and software were hacked, leading to the appropriation of Innovak's customers' social security numbers, addresses, dates of birth and employment information. Innovak was subsequently sued in a putative class action for which it sought coverage under its general liability policy. Innovak's policy contained standard personal and advertising injury language, providing coverage for, among other things, damages relating to the oral or written publication of material that violates a person's right of privacy. The court, in denying coverage, noted that the underlying lawsuit did not allege any "publication" of private information whatsoever; rather, it alleged that hackers *stole* the information. Regardless, even assuming the hacking constituted "publication," the class action did not allege that Innovak—the insured—had published anything, and that publication

[28] Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014).

[29] Innovak Int'l, Inc. v. Hanover Ins. Co., 280 F. Supp. 3d 1340 (2017).

by third-party hackers did not trigger coverage under the policy. At most, according to the court, the complaint alleged that Innovak failed to protect customers' private information by failing to implement necessary data security measures, and this was not the same as alleging "publication."[30]

Likewise, in *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*,[31] the court denied defense coverage to Rosen Hotels following a credit card breach caused by malware installed on the hotel's payment network. The general liability policy at issue covered "personal injury offenses," defined to include "making known to any person or organization covered material that violates a person's right of privacy."[32] Noting that covered personal injuries must result from the *insured's* business activities per the policy, and citing the court's prior decision in *Innovak*, the court denied coverage on the basis that the injuries at issue resulted from the actions of third parties, and not those of the insured.[33]

While case law determining whether data breach coverage constitutes personal or advertising injury continues to evolve, it should be noted that most general liability insurers have expressly eliminated such protection through recent changes to policy forms in efforts to avoid any uncertainly. Current general liability policies typically contain endorsements or other language excluding claims for injury or damages relating to access to, or disclosure of, confidential or personal information. Accordingly, when it comes to data breach and general liability policies, coverage will likely be found only under older policies, notwithstanding the facts or applicable law.

B. Cyber Coverage Under Stand-Alone Cyber Insurance Policies

More recently, and in efforts to address the substantial uncertainty of coverage under traditional general liability and other policies, insurers began marketing and selling insurance policies specifically designed to cover liability stemming from cyberattacks. These so-called stand-alone cyber policies typically offer a broad array of coverages for both liability relating to third-party claims as well as various "first-party"

---

[30] *Id.* at 1347–48.

[31] St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., 337 F. Supp. 3d 1176 (M.D. Fla. 2018).

[32] *Id.* at 1185.

[33] *Id.* at 1185–86.

costs incurred by companies in connection with data breaches and other losses. Cyber policies cover, for instance, costs of defense and settlement of third-party lawsuits relating to cyberattacks, as well as regulatory proceedings and government investigations stemming from privacy breaches. In addition, cyber policies are intended to cover first-party costs, such as the costs of responding to a cyberbreach, including forensic investigation into the cause of the breach, costs of notifying customers of the breach, credit monitoring for customers, data recovery costs and costs associated with public relations and crisis management following an attack. In short, these new cyber insurance policies appear, on their face, to cover most, if not all, of the various types of financial exposures faced by companies in the event of a cyberattack.

But, notwithstanding that stand-alone cyber policies are marketed and sold to provide comprehensive cyber protection, coverage is still far from guaranteed. Indeed, despite broad insuring agreements for an array of risks, insurers faced with claims have raised a host of policy exclusions and other conditions to deny coverage. And, what is more, courts have been relatively receptive to these insurer defenses, as illustrated by the developing case law surrounding cyber coverage claims.

For instance, in *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*,[34] the court denied coverage to P.F. Chang for data breach costs under a cyber policy marketed by Federal as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world."[35] In 2014, hackers obtained and posted on the internet credit card information relating to 60,000 P.F. Chang customers. As a result, P.F. Chang was assessed approximately $2 million in charges by Bank of America Merchant Services, which processed credit card payments made by the restaurant's customers. P.F. Chang sought recovery of these assessments under the Federal policy, which purportedly included express coverage for, among other things, privacy injury and privacy notification and other expenses—the very type of loss incurred by the company. The court, however, held that there was no coverage for P.F. Chang. The policy excluded coverage for loss assumed under contract, as well as costs or expenses incurred by P.F. Chang to perform an obligation assumed under contract without the consent

[34] P.F. Chang's China Bistro, Inc. v. Federal Insurance Company, No. CV-15-1322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).

[35] *Id.* at *1.

of the insurer. Because the assessments at issue were imposed under its contract with a third-party credit card processor (as opposed to the customers themselves), the court held that the exclusions barred coverage.[36] In short, despite having purchased an insurance policy marketed and sold by Federal to cover the "the full breadth of risks associated with doing business in today's technology-dependent world," and purporting to provide express coverage for privacy violations, the court held that under the specific facts of the case, coverage was excluded.

Coverage under a cyber liability policy was likewise denied in *Columbia Casualty Co. v. Cottage Health System*.[37] The matter involved Cottage Health System's claim to recover a $4 million class-action settlement stemming from a data breach. The insurer, however, denied the claim, pointing to a policy exclusion which precluded coverage for claims arising out of the insured's failure to implement certain procedures and risk controls to prevent the cyberattack. While the *Cottage Health System* coverage action was ultimately dismissed on procedural grounds, the case emphasizes another potential issue with coverage under modern cyber liability policies—insurers' refusal to cover claims based on the insured's purported lack of internal controls and procedures designed to prevent data breach.

In sum, while stand-alone cyber policies may afford the most comprehensive insurance available for modern cyberthreats, coverage for any given claim remains fact-dependent and subject to the specific terms of the contract. Not all cyber policies are created equal, and careful negotiation of policy terms and conditions is necessary to secure the most effective coverage.

C. Coverage Under Cyber Endorsements

Short of purchasing a full stand-alone cyber policy, various cyber endorsements are available that can be tacked on to general liability, management liability and other policies to provide protection against cyberthreats. For instance, an Electronic Data Liability endorsement can be added to typical general liability coverage to broaden the scope of covered property damage to include loss of use of electronic data resulting from physical injury to property: "Property damage" means…Loss of, loss of use of,

---

[36] *Id.* at *8.

[37] Columbia Casualty Co. v. Cottage Health System, Case No. LA CV16-03759 JAK (SKx) (C.D. Cal.).

damage to, corruption of, inability to access, or inability to manipulate "electronic data", resulting from physical injury to tangible property…."[38] Similarly, Insurance Services Office's (ISO) Electronic Data Liability Coverage Form covers "those sums that the insured becomes legally obligated to pay because of "loss of electronic data," which is defined to include damage to electronic data.[39] Various manuscript endorsements may also be negotiated that provide cyber coverage beyond these standard ISO forms.

Coverage under a cyber endorsement was recently addressed in *National Ink and Stitch, LLC v. State Auto Property & Cas. Ins. Co.*[40] National Ink and Stitch (NIS) ran an embroidery and screen-printing business, and stored logos, art and designs on its computer system. A ransomware attack prevented access to NIS's data and software, including the art files stored on its server. NIS's computers, however, still functioned, albeit at a slowed pace, and were subject to a dormant virus. NIS's insurance policy covered "physical loss of or damage to Covered Property," while a cyber endorsement amended the definition of "Covered Property" to include "electronic data processing, recording or storage media [and] [d]ata stored on such media."[41]

NIS sought coverage for the costs of replacing its entire computer system; but the insurer denied the claim, arguing that NIS did not sustain "direct physical loss of or damage to" the computer system to justify replacement.[42] The court found coverage based on the plain language of the policy. Distinguishing prior decisions holding that data, which cannot be "touched, held or sensed" and "has no physical substance," is not tangible property under the traditional general liability policy definition of "property damage," the court held that the cyber endorsement expressly included electronic data as "Covered Property."[43] Moreover, the court rejected the insurer's contention that the computer system itself was not covered short of a total inability to function. Rather, the court noted the policy required "physical loss *or damage to*" covered property, which

---

[38] Insurance Services Office General Liability Form No. CG 04 37 04 13 (2012).

[39] Insurance Services Office General Liability Form No. CG 00 65 12 04 (2012).

[40] National Ink and Stitch, LLC v. State Auto Property & Cas. Ins. Co., No. SAG-18-2138, 2020 WL 374460 (D. Md. Jan. 23, 2020).

[41] *Id.* at *1–2.

[42] *Id.* at *2.

[43] *Id.* at *3-4.

was satisfied where the ransomware attack left NIS's computers less efficient and subject to dormant virus attack.[44]

Camp's Grocery, Inc. v. State Farm Fire & Casualty Company[45] is an example of a court adopting a narrow interpretation of a cyber endorsement. Camp's operated a grocery store whose computer network was hacked, compromising customers' private personal data, including credit card information. Camp's was sued by several credit unions which alleged that the data breach, allegedly caused by Camp's inadequate computer system and employee training, caused them to sustain losses, including costs to reissue customer credit cards, transaction fees, and expenses related to their investigation of the matter. Camp's sought defense and indemnity for the lawsuit under two endorsements to its insurance policy that provided coverage for certain computer-related property losses. The forms promised to pay, among other things, "accidental direct physical loss to" computer equipment, removable data storage media, and certain electronic data.[46] The court, however, held that the endorsements did not obligate the insurer to defend or indemnify against the credit unions' claims. Rather, according to the court, "[s]uch promises to pay the insured's 'direct loss' unambiguously afford first-party coverage only and do not impose a duty to defend or indemnify the insured against legal claims for harm allegedly suffered by others, as in third-party coverage."[47]

Here too, as in the case of stand-alone cyber policies, specific endorsement language is key. Companies offered ISO or other boilerplate cyber endorsement are not forced to "take it or leave it." Negotiation of broad coverage through manuscript endorsements may militate against the risk and uncertainly of a court's subsequent interpretation of the policy in the context of a disputed claim.

D. Crime Policies: Computer Fraud and Funds Transfer Fraud

Crime (or fidelity) insurance policies have long existed. While originally designed to protect against traditional business-related financial losses due to employee

---

[44] *Id.* at *5 (emphasis added).

[45] Camp's Grocery, Inc. v. State Farm Fire & Casualty Company, Case No. 4:16-cv-0204-JEO, 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016).

[46] *Id.* at *6.

[47] *Id.*

dishonesty, robbery, forgery, embezzlement, counterfeiting and the like, crime policies have more recently been extended to protect against modern electronic risks, including computer fraud and funds transfer fraud. Typical computer fraud coverage insures against the "direct loss of…money, securities or other property resulting directly from the use of any computer to fraudulently cause a transfer of that property."[48] Similarly, funds transfer fraud protects against loss caused by "an electronic, telegraphic, cable, teletype or telephone instruction" that fraudulently directs a debit or transfer from the insured's account.[49] In recent years, numerous courts have tackled the scope of these coverages in connection with spoofing and other electronic fraud, reaching mixed results for policyholders.

Both computer fraud and funds transfer coverage were considered by a California federal court in *Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of Am.*[50] There, Pestmaster hired a third party, Priority 1, to handle, among other things, payment of Pestmaster's payroll taxes. In connection with the services, Pestmaster executed an Automated Clearing House (ACH) authorization authorizing Priority 1 to initiate ACH transfers from Pestmaster's bank account to Priority 1's bank account. Ultimately, it was discovered that Priority 1 had not used the transferred funds to pay Pestmaster's payroll taxes, but rather, had diverted the money. Pestmaster made a claim for coverage under its crime policy; but the district court determined that the policy afforded no coverage. According to the court, "[t]he Funds Transfer Fraud Insuring Agreement does not cover authorized or valid electronic transactions, such as the authorized ACH transfers in this case, even though they are, or may be, associated with a fraudulent scheme."[51] Nor, according to the court, did the policy's computer fraud insuring agreement cover the loss where the only fraudulent conduct occurred after an authorized transfer of funds had been completed.[52] The Ninth Circuit subsequently affirmed the finding of no coverage, opining: "Because computers are

---

[48] *See, e.g.*, Interactive Communications Int'l, Inc. v. Great Am. Ins. Co., No. 17-11712, 731 Fed. Appx. 929, 931 11th Cir. (May 10, 2018); *see also* ISO CR 00 07 10 90 (2008).

[49] *See* Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of Am., No. CV 13-5-39-JFW, 2014 WL 3844627, at *4 (C.D. Cal. July 17, 2014).

[50] *Id.*

[51] *Id.* at *5.

[52] *Id.* at 7.

used in almost every business transaction, reading [computer fraud coverage] to cover all transfers that involve both a computer and fraud at some point would convert this Crime Policy into a 'General Fraud' Policy."[53]

Relying on *Pestmaster*, a similar result was reached by the Fifth Circuit in *Apache Corporation v. Great American Insurance Company*.[54] There, a fraudulent email caused Apache employees to change a legitimate vendor's payment information and to send invoice payments to a thief's account. The court held that computer fraud coverage was not intended to cover a fraud in which an email was simply part of the scheme. Apache's loss, according to the court, was not a direct result of computer fraud where the transfer of funds was caused by multiple other acts, including a telephone call from the fraudster directing Apache to change vendor account information, a phone call with the thief following the email to confirm the instructions, and review and approval of the transfer by Apache supervisors.[55] To construe the computer fraud insuring agreement so broadly would, in the words of *Pestmaster*, convert the coverage "to one for general fraud."[56]

Pestmaster and *Apache* were later distinguished by a New York federal court in *Medidata Solutions, Inc. v. Federal Ins. Co.*,[57] which found coverage for losses stemming from an email spoofing scheme under both the computer fraud and funds transfer fraud insuring agreements. In *Medidata*, company employees approved several wire transfers in response to fraudulent emails purportedly sent by the company's president. Medidata had purchased a management liability policy from Federal that included a crime coverage section. Federal, however, denied Medidata's claim, arguing that no coverage was afforded under the computer fraud insuring agreement because the "spoofed" emails did not require manipulation of the computer system or input of fraudulent information. Further per Federal, fraud transfer coverage had not been

---

[53] Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of Am., 656 Fed. Appx. 332, 333 (9th Cir. July 29, 2016).

[54] Apache Corporation v. Great American Insurance Company, No. 15-20499, Fed. Appx. 252 (5th Cir. Oct. 18, 2016).

[55] *Id.* at 258.

[56] *Id.*

[57] Medidata Solutions, Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017).

triggered because the wire transfers had been authorized by Medidata employees.[58] The court disagreed on both fronts.

First, distinguishing *Pestmaster*, the court noted that Medidata's computers were indeed manipulated: "[T]he fraud on Medidata was achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identify," and such code "changed data from the true email address to Medidata's president's address to achieve the email spoof."[59] Likewise, in dismissing Federal's argument that the spoofed emails did not "create, authorize, or release a wire transfer" as required by the policy, the court declared that the wire transfers at issue were directly caused by the "thief sending spoofed emails posing as Medidata's president, disagreeing with *Apache* in the process."[60] The court also found coverage under the funds transfer insuring agreement, rejecting Federal's argument that the transfer was voluntarily and knowingly made. Again, the court distinguished *Pestmaster*, recognizing that there, the funds were validly transferred and only later misappropriated. In *Medidata*, in contrast, the employees would not have initiated the transfer but for the thief's manipulation of the emails. "The 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."[61]

More recently, in *American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of Am.*,[62] the Sixth Circuit likewise rejected an insurer's narrow construction of computer fraud coverage as limited to "hacking" and similar incidents in which an ill-intentioned third party gains access or control of the insured's computers. There too, the court held that a spoofing scheme that caused the insured to wire funds to an impersonator triggered coverage for computer fraud. Contrary to Traveler's argument, the policy's

[58] *Id.* at 474–76.

[59] *Id.* at 478.

[60] *Id.* at 479.

[61] *Id.* at 480.

[62] American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of Am., 895 F. 3d 455, 462 (6th Cir. 2018).

definition of "computer fraud" did not require that the fraud "cause any *computer* to do anything."[63]

As indicated by these decisions, the recent trend in case law finds coverage for spoofing-based fraudulent transfers. Computer fraud and funds transfer fraud coverage found in modern commercial crime policies appears, therefore, to provide a valuable protection against this specific cyber risk.

E. Cyber Coverage Under "All Risk" Property Policies

Finally, the Russian NotPetya cyberattacks highlighted in Section II of this Article have given rise to a pair of coverage lawsuits under "all risk" property policies. Much as the name indicates, an "all risk" policy provides first-party property coverage that insures against all risk of loss unless otherwise excluded. Thus, if cyber-related losses are not excluded (which in many instances they are not), these all risk property policies should afford coverage.

The pending lawsuits were filed by Mondelez and Merck, two of the companies hardest hit by the NotPetya attack.[64] The policies at issue in both lawsuits specifically provided enhanced coverage for computer and data-related property damages. The policy sold to Mondelez, for instance, specifically included coverage for "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction…."[65] The Mondelez policy also covered business interruption loss resulting from the failure of Mondelez's electronic data processing equipment or media to operate resulting from malicious cyber damage. Similarly, the policies sold to Merck insured any "destruction,

---

[63] *Id.* at 462 (emphasis added); *see also* Cincinnati Ins. Co. v. Norfolk Truck Center, Inc., 430 F. Supp. 3d 116 (E.D. Va. 2019) (finding coverage under computer fraud insuring agreement where fraudster sent email that caused insured to pay a legitimate invoice to the wrong payee").

[64] *See* Merck & Co., Inc., et al. v. Ace Am. Ins. Co., et al., Case No. UNN-L-002682-18 (N.J. Super. Ct.); Mondelez Int'l., Inc. v. Zurich Am. Ins. Co., Case No. 2018L011008 (Ill. Cir. Ct.).

[65] *Mondelez*, Case No. 2018L011008 (Ill. Cir. Ct.).

or corruption of any computer data, coding, program, or software," and contained a separate insuring agreement for Computer Systems—Non-Physical Damage.[66]

On its face, the coverage sold to Mondelez and to Merck appears to no doubt cover the companies' losses resulting from the NotPetya attacks. Yet, in both instances, the insurers denied the claims based on a single exclusion. The Mondelez policy excluded loss resulting from "hostile or warlike action in time of peace or war." The Merck policy, in turn, contained an exclusion for acts of war or terrorism. According to the insurers, these war exclusions precluded coverage for the NotPetya cyberattacks—a position that, surely, neither Mondelez nor Merck (nor any reasonable insured) would have contemplated as a viable coverage defense to a malware incident.

Both the Mondelez and Merck coverage lawsuits remain pending, and coverage under the respective all risk policies is yet to be judicially determined. But both cases present cautionary tales of the potential limitations of insurance policies for cyber coverage—even those policies specifically designed to cover certain cyberthreats—and of the lengths creative insurers are willing to go to deny coverage for ever-evolving cyber liabilities.

IV. Lessons to Be Learned

Cybercrime is a growing concern for businesses of all types and sizes. And while insurance is often available to mitigate the risk of cyberattack, there are substantial uncertainties surrounding such coverage. While traditional general liability policies may cover some property damage and data breach claims, nowadays most general liability policies contain provisions expressly designed to eliminate such coverage. Commercial crime policies, in turn, may cover certain specific first-party losses such as spoofing-related fraudulent transfers; but these policies do not afford broad protection for the myriad of other potential cyber risks, including third-party liability claims. The recent trend, therefore, is to ensure against data breach and other cyber risks through stand-alone cyber liability policies or endorsements. These are, however, relatively new products, and courts are in the early stages of interpreting cyber policies and rendering opinions regarding the actual scope of coverage which they afford. But it appears clear already, based on cases like *P.F. Chang's Bistro* and *Cottage Health System*, that insurance company marketing of these products may prove to be more hype than substance, and that cyber policies may still contain meaningful gaps in coverage.

---

[66] *Merck*, Case No. UNN-L-002682-18 (N.J. Super. Ct.).

There are several measures companies can take to maximize their insurance coverage for cyber liabilities. First, when considering purchasing a cyber liability insurance policy, it is crucial to carefully and fully assess the potential risks faced—both first-party losses and third-party liabilities—and to understand whether any potential cyber policy is designed to cover such risks. Insurance brokers can put together competing products for consideration, but independent review by coverage counsel is important to fully understand the scope of coverage and to negotiate the broadest coverage provisions available.

Second, in the event of an actual cyber incident, be sure to explore coverage under *all* potential policies, including traditional general liability insurance as well as crime and property policies. Notice should be evaluated under all potential policies, including older "occurrence-based" policies and current "claims-made" policies, which typically require timely notice prior to the policy's expiration. Failure to provide timely notice is an unforced error that can result in forfeiture of coverage.

And, third—perhaps most importantly—if an insurer denies coverage, do not take "no" for an answer. Many insurers aggressively contest valid cyber claims, some asserting exclusions or conditions that were never intended to preclude coverage, as exemplified by the pending NotPetya coverage litigation. Insurance policy interpretation often requires a legal determination whether a claim or loss is or is not covered, and courts, in rendering such a determination, seldom follow insurance industry custom and practice. Skilled coverage counsel can turn an unsupported or improper coverage denial around, either by informal negotiation or through coverage litigation. Companies deserve the benefits of the cyber coverage promised by their insurers.

Tab Turano is Of Counsel at Miller Friel, PLLC, a specialized law firm with the sole purpose of helping corporate clients maximize their insurance coverage. Prior to joining Miller Friel, Mr. Turano worked for more than a decade in the insurance coverage practice group of large law firm. He regularly counsels corporate policyholders on insurance issues and has litigated coverage claims in both federal and state courts around the country. Mr. Turano's expertise in insurance law spans a variety of coverages, including Commercial Property, D&O, Professional Liability, General Liability and Fidelity.