MEALEY'S®
Emerging Insurance Disputes

Email Phishing Scams And Computer Fraud Coverage: Causation Is Key

by
Karen Cestari
and
Bryce Friedman

Simpson Thacher & Bartlett LLP
New York, NY

A commentary article reprinted from the March 19, 2020 issue of Mealey's Emerging Insurance Disputes

LexisNexis®

Commentary

Email Phishing Scams And Computer Fraud Coverage: Causation Is Key

By
Karen Cestari
and
Bryce Friedman

[Editor's Note: Bryce Friedman is a Partner at Simpson Thacher & Bartlett LLP and is based in the Firm's New York office. He advises clients in complex disputes, trials and arbitrations, and devotes a significant part of his practice to representing members of the insurance and reinsurance industries in litigated matters. Karen Cestari is an Attorney at Simpson Thacher & Bartlett LLP and is based in the Firm's New York office. She focuses on insurance and reinsurance law. Any commentary or opinions do not reflect the opinions of Simpson Thacher & Bartlett LLP or LexisNexis®, Mealey Publications™. Copyright © 2020 by Simpson Thacher & Bartlett LLP. Responses are welcome.]

Cybercrime is big business, and showing no signs of slowing down. Companies, both large and small, are falling victim to cyberattacks that frequently result in significant expense. According to one source, cyber-related crimes accounted for approximately $2 trillion in loss last year, and are likely to reach the $6 trillion mark by 2021.[1] Email phishing scams, in particular, have become an increasingly common means for hackers to fraudulently obtain funds from unsuspecting companies. In many such schemes, the target company receives an email from an entity purporting to be from a legitimate source, such as a trusted customer or long-standing vendor. The email, which in actuality is sent from a fraudulent hacker, typically informs the target company that banking or routing information has changed and provides new instructions for upcoming payments. In some scenarios, the email appears to be from a company executive, and directs an employee to follow forthcoming payment instructions relating to a purported company transaction. Hackers have become increasingly sophisticated, such that imposters' email domain names are nearly identical to those of the legitimate parties. By the time the scam is discovered, the fraudulently-induced wire transfers have been effectuated and the devastating financial losses are often unrecoverable. As such, victims of such phishing scams routinely seek insurance coverage for unrecovered losses.

In the past few years, a body of case law that addresses the scope of insurance coverage for such incidents has begun to develop. More specifically, several federal district and appellate courts have addressed the parameters of coverage for phishing schemes under a Computer Fraud provision. This emerging area of insurance law suggests that the determinative issue in many such cyber coverage disputes is the causal connection (or lack thereof) between the use of a computer and the ensuing financial loss. More specifically, courts have focused on whether and under what circumstances a fraudulently-induced wire transfer or other monetary loss is deemed to have resulted "directly" from computer use. As discussed more fully below, when the factual record establishes that one or more intervening steps have occurred between the initial computer contact and the subsequent loss of funds, courts are likely to deny coverage based on the absence of direct causation. Conversely, where the connection between the original phishing email (or other cyber intrusion) and the consequent transfer of funds is deemed direct and uninterrupted, the causation requirement inherent in most Computer Fraud provisions is deemed satisfied.

Computer Fraud Provisions

While specific Computer Fraud provisions vary by policy, most provisions include language requiring direct

causation between the use of a computer and the monetary loss. One common iteration provides coverage for the "loss of . . . money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises . . . [t]o a person . . . outside those premises." Other Computer Fraud provisions cover "loss resulting directly from a fraudulent instruction directing a financial institution to . . . transfer, pay or deliver money or securities." In some policies, the relevant clause requires a "direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud," with "Computer Fraud" defined as "[t]he use of any computer to fraudulently cause a transfer" of money or other property to a third party. Minor variations aside, the common thread in these and other Computer Fraud provisions is the requisite "direct" link between computer use and financial loss. As discussed below, courts' interpretations of the term "direct" under varied circumstances have led to differing conclusions as to the availability of coverage for email phishing schemes.

Cases Finding Coverage

In *Medidata Solutions Inc. v. Federal Ins. Co.*, 729 F. App'x 117 (2d Cir. 2018), an often-cited decision in this context, the Second Circuit ruled that claims arising out of a fraudulent wire transfer were covered by a Computer Fraud provision in the relevant policy. A Medidata employee received an email purportedly sent from the company's president advising her to follow instructions from an attorney regarding a potential corporate acquisition. That same day, a man who identified himself as an attorney called the employee and requested a wire transfer. The employee sought confirmation to make the transfer from Medidata's executives. Thereafter, a group email was sent purportedly from Medidata's president confirming that the wire transfer should be made. After the wire transfer was made, it was discovered that the emails were sent by imposters. Medidata sought coverage under a Computer Fraud provision, among others. A New York district court ruled that coverage was available under the Computer Fraud and Funds Transfer Fraud provisions. *Medidata Sols., Inc. v. Fed. Ins. Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017). In a summary order, the Second Circuit affirmed, ruling that the underlying claims were encompassed by the Computer Fraud provision.

The Computer Fraud provision provided coverage for "direct loss of Money, Securities or Property . . . resulting from Computer Fraud." Computer Fraud, in turn, was defined as the "unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." According to the policy, Computer Violation means "the fraudulent: (a) entry of Data . . . [and] (b) change to Data elements . . . ." As a preliminary matter, the Second Circuit ruled that there was a Computer Violation because the attack constituted both a "fraudulent entry of data into Medidata's computer system," as well as a "change to data" based on the spoofing code that altered the appearance of the email domains.[2] Turning to the causation issue, the Second Circuit ruled Medidata sustained a "direct loss" as a result of the spoofing incident, rejecting the insurer's assertion that the intervening actions by the Medidata employee in effectuating the wire transfer were sufficient to "sever the causal relationship between the spoofing attack and the losses incurred."

The same month that the Second Circuit decided *Medidata,* the Sixth Circuit similarly ruled that claims arising out of wire transfers instigated by fraudulent emails were covered by a Computer Fraud provision. In *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America*, 895 F.3d 455 (6th Cir. 2018), the scheme was initiated by an email purportedly sent by a one of American Tooling's vendors. In actuality, the email was sent by an imposter using an email address with a similar domain. The email instructed American Tooling to send invoice payments to a new bank account. In response, American Tooling wired approximately $800,000 to the account without verifying the new instructions with the vendor. When the fraud came to light, American Tooling sought coverage under the Computer Fraud provision, which covered "direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud." Computer Fraud was defined as "[t]he use of any computer to fraudulently cause a transfer" of money or other property to a third party.

A Michigan federal district court ruled that the insurer owed no coverage because American Tooling's loss was not directly caused by the use of a computer. The court cited the intervening steps that occurred internally at American Tooling between receipt of the fraudulent email and the eventual transfer of funds. *See Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 2017

U.S. Dist. LEXIS 120473, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017). The Sixth Circuit reversed, ruling that American Tooling suffered a "direct loss" of funds when it transferred the money to the imposter. The court explained that the loss was directly caused by computer fraud because the fraudulent email induced a series of internal actions that directly caused the transfer of money. In addition, the Sixth Circuit ruled that the imposter's conduct constituted "computer fraud" because the fraudulent emails and resulting wire transfer were implemented through the use of a computer. Notably, the court rejected the argument that there was no direct loss because American Tooling contractually owed money to its vendor.

More recently, a Virginia federal court followed suit, ruling that losses caused by an email phishing scam were covered by a Computer Fraud provision because the loss resulted "directly" from the use of a computer. *Cincinnati Ins. Co. v. Norfolk Truck Ctr., Inc.*, 2019 U.S. Dist. LEXIS 220076, 2019 WL 6977408 (E.D. Va. Dec. 20, 2019). Norfolk Truck Center received an email from a hacker claiming to be an employee of a company from whom Norfolk purchased supplies. The email provided payment instructions for recent purchases. Over the course of several days, Norfolk completed the necessary filings with its bank and then issued a wire transfer in accordance with the imposter's instructions. When Norfolk discovered that the email was fraudulent, it sought coverage under a Computer Fraud provision, which covered loss "resulting directly from the use of any computer to fraudulently cause a transfer of [money]." The insurer denied coverage, arguing that the loss was not caused "directly" by computer use.

Addressing this matter of first impression under Virginia law, the court ruled that the term "directly," as used in the Computer Fraud provision, was unambiguous and meant "straightforward" or "proximate" and "without intervening agency." Applying this interpretation, the court concluded that the wire transfer loss was caused directly by computer use. The court explained that "[c]omputers were used in every step of the way, including receipt of the fraudulent instructions and the insured's compliance with such instructions by directing its bank to wire the funds to the fake payee." The court rejected the insurer's contention that the loss was not direct because multiple individuals were involved in the wire transfer and because a period of six days elapsed between the initial email and payment. The court also dismissed the argument that coverage was unavailable because Norfolk was attempting to pay a legitimate invoice, rather than a fraudulent bill. The court stated: "the insurance provision does not require a fraudulent payment by computer; rather it requires a computer's use to fraudulently cause a transfer of money."

Employing similar reasoning, the Eleventh Circuit reached the same conclusion in *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, 944 F.3d 886 (11th Cir. 2019). In *Ironshore*, a hacker posing as a company executive sent an email to the company controller. The email stated that the company had been secretly working on a corporate acquisition that would involve a $1.7 million wire transfer to a specific account. The email instructed the employee to await further information from an attorney. Shortly thereafter, someone purporting to be that attorney sent detailed wire transfer instructions. The employee then provided necessary information to its bank in order to effectuate the transfer, including a confirmatory phone call. It was later discovered that the emails were fraudulent. The money was never recovered.

Principle sought coverage under a provision for "[l]oss resulting directly from a fraudulent instruction directing a financial institution to . . . transfer, pay or deliver money or securities." When the insurer denied coverage, Principle sued for breach of contract. A Georgia district court ruled in Principle's favor and the Eleventh Circuit affirmed. As a preliminary matter, the court rejected the assertion that the loss did not involve a "fraudulent instruction," defined as an "electronic or written instruction initially received by [Principle], which instruction purports to have been *issued by an employee*, but which in fact was fraudulently issued by someone else without [Principle's] or the employee's knowledge or consent" (emphasis added). The court deemed it irrelevant that the actual wiring instructions were included in the fraudulent email sent by the imposter attorney (rather than in the email sent by the imposter executive). The court reasoned that the two emails, considered together, constituted a "fraudulent instruction."

Turing to the "resulting directly" requirement, the court reasoned that the term requires proximate causation, and that the employee's interactions with the impersonating attorney and bank did not constitute intervening acts sufficient to break the causal chain. The court also

rejected the contention that proximate causation was a question for a jury, finding that under the factual record presented, the only reasonable conclusion was that the loss "resulted directly from" the fraudulent instruction. The court refused to interpret "directly" as requiring an "immediate" link between the fraudulent instruction and loss.

In *State Bank of Bellingham v. BancInsure, Inc.*, 823 F.3d 456 (8th Cir. 2016), which involved computer hacking rather than email phishing, the causation issue also took center stage. There, a bank's computer system became infected with malware, allowing a criminal to illegally transfer money to a foreign bank account. It was discovered that a bank employee had improperly left security tokens in her computer overnight (in violation of company policy), which left the system vulnerable to attack. The bank sought reimbursement under a financial institution bond, which covered loss "resulting directly" from fraudulent computer activity.

The Eighth Circuit ruled that the fraudulent hacking by criminals, and not the employee's violations of company policy, was the efficient and proximate cause of the loss. The court stated:

> An illegal wire transfer is not a "foreseeable and natural consequence" of the bank employees' failure to follow proper computer security policies, procedures, and protocols. Even if the employees' negligent actions "played an essential role" in the loss and those actions created a risk of intrusion into Bellingham's computer system by a malicious and larcenous virus, the intrusion and the ensuing loss of bank funds was not "certain" or "inevitable." The "overriding cause" of the loss Bellingham suffered remains the criminal activity of a third party.

As such, the court granted summary judgment to the bank on the issue of coverage.

Cases Finding No Coverage

Notably, the year before the Eleventh Circuit issued its decision in *Ironshore*, *supra*, it seemed to endorse a different interpretation of the term "resulting directly" in a cyber coverage case similarly governed by Georgia law. In *Interactive Communications International, Inc. v. Great American Insurance Co.*, 731 F. App'x 929 (11th Cir. 2018), the Eleventh Circuit held that "direct" requires a consequence that follows "straightaway, immediately, and without intervention or interruption."

In *Interactive Communications*, the fraud arose in connection with InComm's debit card services. The company utilized an Interactive Voice Response system (*i.e.*, telephone) in order to allow customers to load funds onto prepaid debit cards issued by banks. In addition to the automated phone system, the funding process also involved computer servers that processed the requested transactions. A vulnerability in InComm's processing center allowed cardholders to add funds to their debit cards in multiples of the amount actually purchased. Before InComm discovered this flaw, unauthorized redemptions caused InComm to transmit more than $11 million to various debit card issuers. InComm sought coverage from Great American for these losses, which the insurer denied.

The Computer Fraud provision covered losses "resulting directly from the use of any computer to fraudulently cause a transfer" of money, securities or other property. A Georgia district court found that the underlying transfers were not caused by "use of a computer" because they were caused directly by the automated telephone system. Although the computer processing system was also involved in the transactions, the court deemed that involvement insufficient to constitute use of a computer. Additionally, the district court held that even if a computer was used, the losses did not "result directly" from computer use because they occurred only after several intervening events: InComm's wire transfer money to a bank; use of the debit card to pay for a transaction; and the bank's payment to the seller for the transaction.

The Eleventh Circuit affirmed the decision. The appellate court disagreed with the district court as to the "use of a computer" ruling, finding that the perpetrators' actions – which involved manipulation of both the telephone and computer systems – constituted use of a computer. However, the Eleventh Circuit affirmed the district court's ruling that the fraud did not "result directly" from use of a computer. Relying on the "plain meaning" and dictionary definition, the court held "directly" requires a consequence that follows "straightaway, immediately, and without intervention

or interruption." The court concluded that this standard was not met because of the time lapse and intervening steps between the computer fraud and the loss, including the transfer of funds onto the debit cardholders' accounts and the purchase of goods by individual debit cardholders. Incomm argued that the loss was immediate because it occurred at the moment the funds were improperly transferred to the debit cardholders' accounts. The court disagreed, noting that Incomm retained some control over the funds at that point and could have prevented the loss by stopping distribution of the money from the account to the merchants. Instead, the court explained, the loss occurred when funds were disbursed to the merchants for purchases made by cardholders, because at that point, Incomm could not recover the funds.

In *Apache Corp. v. Great American Insurance Co.*, 662 F. App'x 252 (5th Cir. 2016), cited by the Georgia district court in *Interactive Communications* and involving an identical Computer Fraud provision, the Fifth Circuit denied coverage for wire transfers initiated by fraudulent emails. The fraud was initiated by a telephone call to Apache from a person identifying herself as a Petrofac representative (a vendor for Apache). The caller instructed Apache to change the banking information for future payments. The Apache employee replied that the change could not be processed without a formal request on Petrofac letterhead. Thereafter, Apache received an email from an address created by criminals to closely resemble Petrofac's email address. The email attached a letter on fraudulently-created Petrofac letterhead confirming the request to change the bank account. Apache called the telephone number provided in the letter to confirm the change and then approved the change. After nearly $7 million in payments were made to the new bank account, Apache discovered that the phone call and email came from criminals. Apache sought coverage from Great American, which denied coverage on the ground that the loss did not "result directly from the use of a computer," as required by the policy.

Addressing this matter of first impression under Texas law, the Fifth Circuit ruled that the Computer Fraud provision did not cover Apache's claims because the loss resulted from a series of events and was not "directly" caused by computer use. In particular, the court reasoned that the wire transfers resulted from a sequence of actions and circumstances, including the criminals' initial phone call, the subsequent phone call to the fraudulent phone number, and Apache's insufficient internal controls for account changes. The court stated:

> The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process, would . . . convert the computer-fraud provision to one for general fraud.

The Fifth Circuit noted that Computer Fraud provisions are intended to have limited application to claims arising directly out of use of a computer (such as hacking) and do not extend to fraud claims that merely involve use of a computer at some point in the transaction.

In some cases, courts have rejected policyholder attempts to obtain Computer Fraud coverage based on a different issue. Some Computer Fraud provisions require "fraudulent entry" into a computer or entry by an "unauthorized user." When such language is presented, courts have ruled that loss caused by the actions of an authorized company employee are not covered, even when those actions were the result of a fraudulent email or other criminal scheme. For example, in *Taylor & Lieberman v. Federal Insurance Corp.*, 681 F. App'x 627 (9th Cir. 2017), the Ninth Circuit ruled that there was no Computer Fraud coverage for an email phishing scheme that resulted in a wire transfer to criminals. The court reasoned that "there is no support for [the] contention that sending an email, without more, constitutes an unauthorized entry into the recipients computer system," as required by the policy. The court further held that fraudulent emails instructing the policyholder to effectuate the wire transfers do not amount to an "introduction of instructions" that "propogate[d] themselves" through the computer system. The court reasoned that those policy terms refer to malicious computer codes and other similar intrusions.[3]

The Ninth Circuit again addressed the issue of authorized computer entry in *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of America*, 719 F. App'x 701 (9th Cir. 2018), although this time relating to application of a policy exclusion. There, the court assumed, without deciding, that wire transfer losses initiated by

a fraudulent email were covered by a Computer Fraud provision. However, the court ruled that coverage was barred by an exclusion that applied to "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." The court reasoned that the exclusion squarely applied because the employees that changed the payee information in the company's computers (albeit as a result of a fraudulent "spoofed" email) were authorized to enter the computer system and because the losses at issue were caused by the payment changes made by those authorized employees.

In *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh,* 37 N.E.3d 78 (N.Y. 2015), the New York Court of Appeals similarly focused on the "fraudulent entry" issue, albeit under a distinct factual scenario. Universal, a health insurance company, incurred more than $18 million in losses for payment of fraudulent medical services that were never actually performed. Those payments were processed and made via computer. The Computer Systems Fraud clause in Universal's policy provided indemnification for "Loss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program . . . ." The court ruled that coverage for the "fraudulent entry" of data is limited to losses caused by unauthorized access into the policyholder's computer system (such as intrusions by hackers) and did not encompass losses caused by an authorized user's submission of fraudulent information into the computer system.

In one case, Computer Fraud coverage was deemed inapplicable to an email phishing scheme/wire transfer scenario based on verbiage relating to physical loss. In *Rainforest Chocolate, LLC v. Sentinel Insurance Co., Ltd.*, 204 A.3d 1109 (Vt. 2018), the Computer Fraud provision was expressly limited to "physical loss of or physical damage to money . . . resulting from computer fraud." Emphasizing the requisite physical loss, the Vermont Supreme Court ruled that the provision did not encompass a (non-physical) wire transfer loss.

The Forgery Provision

Although Computer Fraud provisions have been the most frequent focus of emerging cyber coverage litigation, several decisions have addressed the scope of coverage under Forgery provisions for losses stemming from cyber scams.

In *Taylor & Lieberman*, *supra,* the Ninth Circuit not only rejected Computer Fraud coverage for losses caused by email phishing, but also ruled that the Forgery provision was inapplicable. The Forgery provision protected against direct loss "resulting from Forgery or alteration of a Financial Instrument by a Third Party." The court concluded that this language extended coverage only to the forgery of a financial instrument, and did not encompass a fraudulent email.

Faced with different policy language, the Eleventh Circuit also denied Forgery coverage for computer-initiated losses in *Metro Brokers, Inc. v. Transportation Insurance Co.*, 603 F. App'x 833 (11th Cir. 2015). The Fraud and Alteration Endorsement at issue provided coverage for loss resulting directly from "forgery," defined as "the signing of the name of another person or organization with intent to deceive." The court ruled that this provision did not cover the losses at issue because the electronic fund transfers did not involve any of the written instruments listed in the endorsement and did not involve the signing of a name. Further, the court held that the use of stolen passwords and identification numbers is not equivalent to the signing of another person's name.

In a case involving a Forgery and Alteration provision identical to that in *Metro Brokers*, the Indiana Court of Appeals similarly declined to find coverage for computer hacking losses. In *Metal Pro Roofing, LLC v. Cincinnati Insurance Co.*, 130 N.E.3d 653 (Ind. Ct. App. 2019), the court emphasized the lack of evidence that the hacker "signed" any document, "let alone that they signed 'the name of another person or organization.'" The court stated: "using a computer to hack into someone else's bank account to steal money clearly involves wrongful conduct. However, by arguing that it involves 'forgery' or 'alteration' . . . the [policyholders] are attempting to put a square peg in a round hole."

In *Medidata, supra,* a New York district court held that coverage was not available under a Forgery provision. Although the court did find that the losses were encompassed by Computer Fraud and Funds Transfer Fraud provisions, it concluded that absent alteration of a financial instrument, there could be no Forgery coverage. The court declined to rule on whether spoofed emails containing Medidata's president's name constituted a forgery, noting that even if they did, the lack of a financial instrument was fatal to coverage under the Forgery clause.

What's Next? The Future of Coverage Litigation For Cyber Crime Losses

Cyberattacks, email phishing schemes and other incidents of social engineering that result in losses to companies continue to proliferate at an alarming rate. Undoubtedly, courts will be called upon to address the parameters of coverage under first-party and general liability policies, as well as specific cybercrime policies for various incidents of cyber fraud.

In addition to the emerging body of law that has developed in the context of Computer Fraud and Forgery provisions, novel questions of insurance coverage law that implicate other coverage or exclusionary clauses will also likely arise. Future cyber-related coverage litigation is likely to require interpretation of conventional policy terms in the context of unconventional factual scenarios.

A recent Virginia district court opinion illustrates this point. In *Quality Plus Services, Inc. v. National Union Fire Insurance Co. of Pittsburgh*, 2020 U.S. Dist. LEXIS 7337, 2020 WL 239598 (E.D. Va. Jan. 15, 2020), the court addressed a number-of-occurrences dispute and application of a "Territory Condition" in a case involving an email phishing scam. There, a Quality Plus employee received five emails, purportedly from the President of the company, that instructed her to make wire transfers to banks in Mexico and Hong Kong. After the payments were made, Quality Plus discovered that the emails were fraudulent. The company sought coverage under a Funds Transfer Fraud provision that contained a $1,000,000 per-occurrence limit with a $10,000 deductible. The insurer denied coverage on several bases, including a Territory Condition, which limited coverage to loss "resulting directly from an Occurrence taking place within the United States of America." The court ruled that the operative "occurrence" was the sending of the emails by the criminals, but concluded that a disputed issue of fact existed as to whether the emails were sent from a location within the United States. Although the emails' IP addresses suggested that they were sent from Nigeria, the court acknowledged the possibility that those addresses were fabricated. In addition, testimony relating to a telephone conversation with one of the hackers also raised questions as to whether the emails were sent from a foreign country.

The court also ruled that issues of fact existed as to the number of occurrences for purposes of applying the per-occurrence limit. In particular, the parties disputed whether one person or multiple individuals sent the fraudulent emails. This determination controls the amount of damages, if any, awardable to Quality Plus because the policy defines "Occurrence" as an act or event, or combination or series of acts of events "committed by the same person acting alone or in collusion with other persons." The court ruled that the question of whether the loss was caused by five occurrences or one occurrence must be decided by the finder of fact, based on evidence relating to differences between and/or similarities among the five emails, among other things.

In addition to the number-of-occurrence and covered territory issues raised in *Quality Plus*, several other substantive issues are likely to arise in future cyber-coverage litigation, including the following:

Is There Covered Property Damage?

As disruptions to and corruptions of software programs, data files and other computer systems continue to result from hacking and other cyber fraud activity, disputes may arise as to whether there has been covered property damage. In *National Ink & Stitch, LLC v. State Auto Property & Casualty Co.*, 2020 U.S. Dist. LEXIS 11411, 2020 WL 374460 (D. Md. Jan. 23, 2020), the court ruled that the policyholder's loss of data and impairment to its computer system, resulting from a ransomware attack, constituted "direct physical loss" under a business owner's policy. That decision turned largely on an endorsement that specifically covered electronic media and records, and thus may have limited application to cases involving policies without such clauses. The court also addressed the question of whether a complete and total loss of use is required in order to satisfy "direct physical loss." The court held that where a policy does not define "direct physical loss" to specifically require a complete inability to use a computer system, no such requirement will be implied. As *National Ink* demonstrates, governing policy language will be of critical importance in this context.

Do Exclusions Bar Coverage?

Certain policy exclusions may operate to bar coverage for otherwise covered cyber-related losses. Exclusions pertaining to acts of war or terrorism may be invoked in cases involving actions by foreign governments or

entities deemed to be acting on behalf of such governments. In addition, professional services exclusions may be implicated when underlying litigation involves insured companies in the business of providing cybersecurity or other computer services.[4] Furthermore, exclusions arising out of contract may come into play where claims arise out of or involve a contract between the policyholder and a third-party relating to cyber security or other computer services. Finally, as insurers begin to include policy exclusions that relate specifically to computer fraud, such exclusions may serve as a clear bar to coverage for email phishing scheme losses. This was precisely the case in *Tidewater Holdings, Inc. v. Westchester Fire Insurance Co.*, 389 F. Supp. 3d 920 (W.D. Wash. 2019). There, the court assumed, without deciding, that the wire transfer loss was covered by a Computer Fraud provision, but held that coverage was nonetheless barred by a Fraudulent Transfer Request Exclusion, which stated that "the Insurer shall not be liable for any loss resulting from any Fraudulent Transfer Request."

The specific wording of an exclusion is likely to be outcome-determinative in cases involving email phishing schemes, as illustrated by *Rainforest Chocolate*, *supra*. There, the Vermont Supreme Court ruled that a False Pretense Exclusion, which applied to the "voluntary parting" with property if induced to do so by fraud or false pretense, was ambiguous as to whether it applied only to physical loss or also to the loss of funds. The court therefore declined to enforce the exclusion to bar coverage for the company's wire transfer loss.

Has Private Information Been 'Published'?

Numerous incidents of cybercrime involve the taking of confidential or private customer information, rather than the transfer of funds. In such instances, policyholders are likely to seek liability coverage for losses stemming from those data breaches pursuant to a Personal and Advertising Injury provision. This coverage, distinct from bodily injury or property damage coverage, is often limited to a specific list of offenses, including the "oral or written publication, in any manner, of material that violates a person's right to privacy." To the extent that this provision is the subject of coverage litigation, courts will be required to decide several key issues, including the following: (1) what information is deemed "private"?; (2) has there been a "publication"?; and (3) who is responsible for any such publication, the policyholder or a third-party?[5]

Other Factors That May Affect Potential Coverage

As with any insurance coverage dispute, an insurer's extra-contractual conduct might affect coverage. In one recent decision, an insurer's explicit reference to "computer hackers" in its promotional material gave rise to a potential for coverage by estoppel. In *Metal Pro Roofing, supra*, the court ruled that losses caused by computer hackers were not covered by several provisions in a crime policy, but that coverage might nonetheless be implicated based on language contained in the insurer's quotes and accompanying materials. Such language included references to "money and securities" and "computer hackers." Although the materials contained a disclaimer that the statements did not constitute a statement of coverage, the court ruled that the coverage determination would turn on resolution of disputed issues of fact relating to reasonable reliance on the promotional materials.

Endnotes

1. https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/

2. In so ruling, the court distinguished the New York Court of Appeals decision in *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh,* 37 N.E.3d 78 (N.Y. 2015). As discussed *infra*, *Universal* involved fraudulent medical bills that were inputted into a health care company's computer system by an authorized employee.

3. The court also deemed a Funds Transfer Fraud provision inapplicable because it required transfers to be made "without an Insured Organization's knowledge or consent." Here, the policyholder knew about the wire transfers and directed the transfer of funds after receiving the fraudulent emails.

4. In a recent decision, a New York district court ruled that coverage for losses resulting from an email phishing scam was not barred by an otherwise applicable "Modified Investment Advisor Exclusion Endorsement" because of an exception to the exclusion for claims arising out of the insured's "professional services." *SS&C Tech. Holdings, Inc. v. AIG Specialty Ins. Co.*, 2020 U.S. Dist. LEXIS 17201, 2020 WL 509028 (S.D.N.Y. Jan. 31, 2020).

5. A few courts have addressed these issues in cases involving both intentional hacking and the accidental loss of data. *See Am. Econ. Ins. Co. v. Hartford Fire Ins. Co.*, 695 F. App'x 194 (9th Cir. 2017) (installation of spyware on users' computers to monitor keystrokes and take pictures did not satisfy "publication" requirement absent allegations of transmission of material to third party); *Innovak Int'l, Inc. v. The Hanover Ins. Co.*, 280 F. Supp. 3d 1340 (M.D. Fla. 2017) (release of personal private information caused by data breach is not a "publication" if it was not sent to a third party, and alternatively, publication would not be satisfied if material was published by hackers rather than the policyholder); *Total Recall Information Mgmt, Inc. v. Federal Ins. Co.*, 2015 WL 2371957 (Conn. 2015) (loss of computer tapes containing personal information during transportation does not satisfy "publication" requirement). ■

MEALEY'S: EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 1087-139X