

Cyber Risk and Insurance: Does Commercial Crime Insurance Cover Email Spoofing?

November 16, 2018

Client Advisory

November 16, 2018 by Mark R. Zancolli, H. Thomas Davis, Jr., John M. Griem, Jr. and Matthew B. James

This is the second of four Client Advisories concerning cyber risk and insurance. The [first Advisory](#) discussed the limited protection which traditional commercial general liability (“CGL”) insurance provides for losses from cybersecurity incidents. This second Advisory discusses claims under commercial crime insurance, focusing primarily on claims for losses resulting from social engineering fraud involving email “spoofing” scams. Subsequent Advisories will discuss the limitations of some cyber insurance policies, as well as items to consider when purchasing cyber insurance.

The theme of these Advisories is that a business that relies solely on traditional insurance such as a CGL policy to cover cyber risks is likely in for an unpleasant surprise, and that language in a cyber insurance policy can provide its own unfavorable surprises unless thoughtfully reviewed, negotiated and drafted.

Introduction: Email Spoofing and Computer Fraud

In recent years, cyber criminals have developed increasingly sophisticated cyber attack methods to steal money from businesses. One such attack vector that has become widespread is social engineering fraud through email spoofing scams (also known as “business email compromise” and “fraudulent instruction” schemes), in which a thief disguises an email to make it appear to come from a person from whom it did not originate for the purpose of inducing the email’s recipient to transfer funds to an account controlled by the thief. Some commentators have noted that these types of attacks often occur at times when businesses and their employees can tend to be less vigilant, such as on a Friday afternoon.

Email spoofing scams have received considerable attention in recent publications and crime statistics. Last month, the SEC issued a cautionary report regarding two types of email spoofing scams — the first involving emails from persons purporting to be executives of the targeted company requesting that company funds be wire transferred to a foreign bank account controlled by the impersonator, and the second involving emails from persons purporting to be representatives of a vendor requesting that the targeted company wire transfer payments owed to the vendor to foreign bank accounts controlled by the impersonator (as discussed in our October 29, 2018 [Advisory](#)). **Additionally, according to the FBI’s 2017 Internet Crime Report, the FBI’s Internet Crime Complaint Center (“IC3”) received 15,690 “business email compromise” / “email account compromise”[1] complaints in 2017, with adjusted losses of over \$675 million – the highest loss total of all the crime types listed in the Report.[2]**

Many businesses that have suffered a loss resulting from an email spoofing scam have submitted a claim to their insurer seeking coverage for the loss under their crime insurance policy, and many insurers have denied such claims. Insureds have most often sought coverage for such losses under their policy’s “Computer Fraud” provision, which typically states that the insurer will pay for the insured’s “direct loss” caused by

"computer fraud," defined in many such policies as "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the [insured's] Premises or Financial Institution Premises . . . to a person [or a place] outside the Premises or Financial Institution Premises," or similar language. Many insurers that have denied coverage for such claims have asserted that the insured did not suffer a "direct loss" caused by computer fraud, contending that the loss was not directly caused by the impersonator's spoofed email but was instead caused by the intervening actions of the insured's employees who transferred the lost funds to the impersonator's account. Insurers have also argued that Computer Fraud coverage applies to "hacking-type intrusions" where a fraudster gains access to an insured's computer system to perform the transfer from the insured to the fraudster, and that email spoofing scams are therefore not covered because they do not entail the fraudster's gaining access to the insured's computers to perform the transfer. Insurers also have denied coverage for such claims based on a number of policy exclusions, including exclusions for transfers made by an authorized person or resulting from the input of electronic data by a person authorized to enter the insured's computer system.

Lessons for Companies Drawn from Court Decisions

Court cases involving disputes as to coverage for email spoofing losses under crime policies have had mixed outcomes. Although the recent *Medidata* and *American Tooling* decisions (discussed below) may assist certain insureds in obtaining coverage for email spoofing losses under the Computer Fraud provisions of their crime policies, the case law demonstrates that even slight variations in language from one insurance policy to another can be crucial in a court's determination as to whether or not a loss is covered. Two lessons can be drawn from these cases. First, it is important that businesses obtain policies containing language covering the social engineering fraud risks that they face in their specific business. Second, a business's accounts payable and financial control personnel should be rigorously trained to never rely on instructions provided in an email from a company executive, attorney, vendor or client to make a wire transfer to an account that has not been previously verified, or to change bank account wiring information for future payments, without first confirming the instructions directly with the company executive, attorney, vendor or client (as the case may be) using previously verified contact information.

Specific coverage for social engineering fraud is now offered by several crime insurers, and a number of insurers now also offer add-on endorsements, to cyber and crime policies, that are specifically designed to apply to losses from social engineering fraud. **Businesses should therefore consult with an experienced insurance broker and legal counsel to explore coverage options and review policy language when evaluating and purchasing coverage for computer fraud and social engineering fraud.**

Recent Decisions Favoring Insureds

This past July, the U.S. Court of Appeals for the Second Circuit, applying New York law, affirmed a New York district court's decision in favor of the insured in a coverage dispute under crime insurance for loss resulting from an email spoofing incident. In that case, entitled *Medidata Solutions, Inc. v. Federal Ins. Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 Fed. Appx. 117 (2d Cir. 2018), an accounts payable employee of the insured received a spoofed email purportedly from the insured's president – with the president's name, email address and photo appearing in the "From" field of the email – stating that the insured was close to finalizing an acquisition and instructing the accounts payable employee to devote her full attention to the demands of an attorney who would be contacting her. A person who held himself out to be the attorney proceeded to telephone the accounts payable clerk and requested that she process a wire transfer for him. After the accounts payable employee informed the purported attorney that she needed an email from the insured's president to process the wire transfer, another spoofed email purportedly from the insured's president was received by the accounts payable employee and the insured's vice president and director of revenue, instructing them to process and approve the wire transfer. They proceeded to wire transfer approximately \$4.8 million to a bank account that was provided by the purported attorney, and not until two days later did the insured realize that it had been defrauded and that the transferred funds were lost. 268 F. Supp. 3d at 473-474.

The insured sought coverage for the loss under the Computer Fraud Coverage provisions of its “Executive Protection” policy’s Crime Coverage section, which covered the “direct Loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party.” The policy defined “Computer Fraud” as “the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation,” including “the fraudulent (a) entry of Data into . . . a Computer System; [and] (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format . . . directed against an Organization.” The insurer denied coverage for the loss, contending that there had been no fraudulent entry of data into the insured’s computer system, that the spoofed emails did not cause any fraudulent change to data elements or program logic of the insured’s computer system, that the policy only applies to “hacking-type intrusions,” and that the insured did not sustain a “direct loss” as a result of the spoofing attack. The Second Circuit rejected the insurer’s arguments and affirmed the district court’s grant of summary judgment in favor of the insured, finding that there was a fraudulent entry of data into the insured’s email system – which constituted a “computer system” within the meaning of the policy – since the spoofing code embedded in the emails made them appear to come from the insured’s president. The court further found that there was a change to a data element within the meaning of the policy since the email system’s appearance was altered by the spoofing code to misleadingly indicate the sender. Significantly, the court also rejected the insurer’s argument that the insured had not suffered a “direct loss” as a result of the spoofed emails, finding that the spoofing attack was the proximate cause of the insured’s losses and that the actions by the insured’s employees to effectuate the transfer of funds was insufficient to sever the causal relationship between the spoofed emails and the insured’s loss. 729 Fed. Appx. at 118-119.

In another decision issued in July just a week after the *Medidata* decision, the U.S. Court of Appeals for the Sixth Circuit, applying Michigan law, reversed an earlier Michigan district court decision in favor of an insurer and granted summary judgment in favor of the insured on the insured’s claim for coverage under a policy’s computer fraud provision for loss resulting from an email spoofing incident. In that case, entitled *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017), *rev’d*, 895 F.3d 455 (6th Cir. 2018), the insured’s treasurer sent an email to a vendor to which the insured outsourced some of its manufacturing work, requesting that the vendor provide copies of all outstanding invoices for work that the vendor had performed for the insured. An unidentified third-party intercepted that email and responded to it by sending the insured’s treasurer a spoofed email which purported to be from the vendor and instructed the insured to send payment for several legitimate outstanding invoices to a new bank account. After the insured verified that the vendor had met certain production milestones, the insured wire transferred approximately \$800,000 to the bank account specified in the spoofed email without verifying the bank account change with the vendor. 2017 WL 3263356 at *1. When the real vendor demanded payment of the outstanding invoices, the insured realized the fraud and that the bank account to which the funds had been transferred was not controlled by the vendor, but the transferred funds could not be retracted. The insured paid the vendor approximately 50% of the outstanding debt and agreed that the remaining 50% would be contingent on the insured’s insurance claim. 895 F.3d at 458.

The insured sought coverage for the loss under the Computer Fraud provision of its business insurance policy’s Computer Crime section, which covered “the Insured’s direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud,” which the policy defined as “[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Financial Institution Premises . . . to a person (other than a Messenger) [or to a place] outside the Premises or Financial Institution Premises . . . ” In granting summary judgment for the insured and reversing the district court’s grant of summary judgment for the insurer, the Sixth Circuit rejected the insurer’s contentions that there was no coverage because the insured did not suffer a “direct loss,” because the insured’s loss did not constitute “Computer Fraud,” and because the loss was not “directly caused by Computer Fraud” within the meaning of the insured’s policy. Regarding the insurer’s assertion that the insured did not suffer a “direct loss” within the meaning of the policy, the insurer contended that the loss did not arise when the insured paid the imposter – because the insured had already contracted with the vendor to pay that money for the product it had received – but rather that the loss arose later, after the fraud was discovered, when the insured agreed to pay the vendor at least half of the money still owed. The court rejected that argument, finding that the insured suffered a “direct loss” when it

transferred the funds to the imposter, and that the fact that the insured owed that money to the vendor and later agreed with the vendor to spread the loss between them had no bearing on whether the loss was directly suffered by the insured. *Id.* at 459-461.

Regarding the insurer's contention that the insured's loss did not constitute "Computer Fraud" within the meaning of the policy, the insurer argued that "Computer Fraud" requires a computer to fraudulently cause the transfer and that it is insufficient to simply use a computer and have a transfer that is fraudulent. In making that argument, the insurer relied on a decision issued by the Ninth Circuit Court of Appeals in a case entitled *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 Fed. Appx. 332, 333 (9th Cir. 2016), which interpreted the phrase "fraudulently cause a transfer" in a policy's Computer Fraud provision to require "an unauthorized transfer of funds" and which further stated that "because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert the Crime Policy into a 'General Fraud' Policy." However, the court found *Pestmaster* to be factually distinguishable since the fraudulent conduct in that case occurred without the use of a computer since the payroll tax vendor hired by the insured in that case – who had been authorized by the insured to electronically access the insured's bank account to pay the insured's payroll taxes – transferred funds out of the insured's account as authorized but kept the funds to pay its own obligations instead of paying the insured's payroll taxes. By contrast, the court found that, unlike in *Pestmaster*, the insured's loss did result from "Computer Fraud" since the imposter sent emails to the insured using a computer and those emails fraudulently caused the insured to transfer money to the imposter. Further, the court stated that the insurer's "attempt to limit the definition of 'Computer Fraud' to hacking and similar behaviors in which a nefarious party somehow gains access is not well-founded." 895 F.3d at 461-462.[3]

Decisions Favoring Insurers

As noted above, court decisions in cases involving claims for coverage under crime policies for social engineering fraud have been mixed, and, prior to the *Medidata* and *American Tooling* decisions discussed above, the vast majority of decisions addressing such claims favored insurers. One such case is the Fifth Circuit Court of Appeals' decision in *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016). In that case, an employee of the insured received a telephone call from a person falsely claiming to be a representative of one of the insured's vendors. The caller requested that the insured change the bank account information for payments to be made to the vendor. The insured's employee told the caller that the change request needed to be submitted on the vendor's letterhead, and, a week later, the insured's accounts payable department received an email from a slightly different domain address than the vendor's email domain. Attached to the email was a signed letter on the vendor's letterhead (altered to include a phone number different than the vendor's phone number) purporting to contain new bank account details for making payments to the vendor. An employee of the insured called the number on the letterhead to verify the request, and another employee of the insured approved the changed bank account details. The insured proceeded to transfer funds to the new account for payment of the vendor's invoices, and less than a month later, the insured was notified that the vendor had not received the approximately \$7 million that the insured had transferred to the fraudulent bank account. *Id.* at 253.

After an investigation of the crime enabled the insured to recoup a portion of the transferred funds, the insured submitted a claim for the remaining balance to its insurer under the Computer Fraud provision of a crime protection policy, which stated in relevant part that the insurer "will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: a. to a person (other than a messenger) outside those premises; or b. to a place outside those premises." The insurer denied coverage for the claim, asserting that the loss was not covered because the email did not "cause a transfer" within the meaning of the Computer Fraud provision and that coverage under that provision is limited to losses from "hacking and other incidents of unauthorized computer use." In granting summary judgment for the insurer and reversing an earlier Texas district court decision in favor of the insured, the Fifth Circuit, applying Texas law, held that the loss did not directly result from the use of a computer, finding that the fraudulent email "was merely incidental to the occurrence of the authorized transfer of money" and that "the authorized transfer was made to the fraudulent account only because, after receiving the email, [the insured] failed to investigate accurately the new, but fraudulent, information provided to it." The court further cited *Pestmaster* for the proposition that "[t]o 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." *Id.* at 254-255.

Likewise, the Ninth Circuit Court of Appeals, applying California law, affirmed a California district court's decision denying coverage under a crime policy for loss resulting from a social engineering scam in the case of *Taylor and Lieberman v. Federal Ins. Co.*, 2015 WL 3824130 (C.D. Cal. 2015), *aff'd*, 681 Fed. Appx. 627 (9th Cir. 2017). In that case, the insured, an accounting firm, received an email from one of its clients requesting that approximately \$94,000 be wire transferred from the client's account (over which the insured had management responsibility pursuant to a power of attorney, including with regard to transferring funds) to an account at a bank in Malaysia. The client's name was typed at the end of the email, but the email was sent by an unauthorized third-party who had gained control over the client's email account. The insured's employee who received the email believed that the instructions were from the client, so she arranged for the wire transfer and sent a confirmation email to the client. The following day, the insured's employee received another email from the client's email address with the client's name typed at the end, requesting that an additional amount of approximately \$98,000 be wire transferred to an account in Singapore, and the insured's employee once again arranged for the wire transfer and sent a confirmation to the client's email address. Thereafter, the insured's employee received a third email, purportedly from the client but from a different email address than the first two emails, requesting that an additional amount of approximately \$128,000 be wire transferred to another account in Malaysia. The fact that the third email came from a different email address than the first two prompted the insured's employee to call the client to confirm whether the client had sent it, at which point the employee discovered that the emails were fraudulent.

Although the insured tried to recoup the transfers, it was only able to retrieve a portion of the amount of the first one. The insured complied with the client's subsequent request to repay the lost funds, and then it submitted a claim to its insurer seeking reimbursement of the lost funds under the Computer Fraud, Forgery and Funds Transfer Fraud provisions of its insurance policy. The district court determined that because each of those policy provisions states that they apply to "direct loss sustained by an Insured," they did not provide coverage for the lost funds since they only provide coverage for fraudulent violations that result in a "direct loss" of the insured's own money, and not for fraudulent violations that result in a loss of a third party's (i.e., the client's) money for which the insured seeks reimbursement from the insurer. 2015 WL 3824130 at *3-4. On appeal, the Sixth Circuit affirmed the district court's denial of coverage and further rejected the insured's contention that the Computer Fraud provision applied because the emails constituted an unauthorized "entry into" its computer system, as well as an unauthorized "introduction of instructions" that "propagate[d] themselves" through its computer system, within the meaning of the policy. In that regard, the court stated that there was no support for the insured's contention "that sending an email, without more, constitutes an unauthorized entry into the recipient's computer system," and that the emails were not an unauthorized introduction of instructions that propagated themselves through the insured's computer system, such as malicious code. 681 Fed. Appx. at 629.[4]

In another case decided by the Ninth Circuit Court of Appeals involving a claim under a crime insurance policy for loss resulting from a social engineering scam, the court affirmed a Washington district court's decision in favor of the insurer and held that coverage was barred by a policy exclusion for loss resulting from an authorized person's input of electronic data into the insured's computer system. In that case, entitled *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co.*, 2016 WL 3655265 (W.D. Wash. 2016), *aff'd*, 719 Fed. Appx. 701 (9th Cir. 2018), the insured, an importer of seafood, purchased frozen shrimp from a vendor whose computer system was hacked. The hacker intercepted email exchanges between the insured and the vendor, and then sent fraudulent emails to the insured using spoofed email domains that were altered to appear similar to the vendor's employees' emails (such as by substituting the number "1" with a lower case "l"). In those emails, the hacker requested that the insured change the bank account information for future wire transfers to the vendor. The insured's treasury manager entered the new bank account information in a spreadsheet on the insured's computer system, and a hard copy of that spreadsheet was included in a package of documents provided to the insured's management for approval of payments to vendors. The insured's treasury manager used information from that spreadsheet to prepare and initiate wire transfers to the account for which the hacker had emailed wire instructions, and the insured was ultimately defrauded of approximately \$713,000 by the hacker. 2016 WL 3655265 at *1-3.

The insured submitted a claim for the loss to its insurer under its crime policy's Computer Fraud provision, which provided that the insurer "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." The Computer Fraud provision was subject to an exclusion, "Exclusion G," upon which the insurer relied to deny coverage and which stated that the policy "will not apply 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." Applying Washington law, the Ninth Circuit ruled that, even assuming — without deciding — that the insured's loss was covered under the policy's Computer Fraud provision, coverage for the loss was excluded by Exclusion G since the insured's employee had "the authority to enter" the insured's computer system when she "input" electronic data on that computer system, which changed the wiring information for the vendor and resulted in the funds being wire transferred to the hacker's account. 719 Fed. Appx. at 702.

Next Client Advisory in this series: Cyber Insurance

For more information concerning the matters discussed in this publication, please contact the authors **Mark R. Zancolli** (212-238-8735, zancolli@clm.com), **H. Thomas Davis, Jr.** (212-238-8850, davis@clm.com) **John M. Griem, Jr.** (212-238-8659, griem@clm.com), **Matthew James** (212-238-8644, james@clm.com) or your regular Carter Ledyard attorney.

[1] "Email account compromise" is a variation of business email compromise that targets individuals who regularly perform wire transfer payments. See FBI, 2017 Internet Crime Report, at 12.

[2] See FBI, 2017 Internet Crime Report, at 12, 21.

[3] Another case in which a court ruled in favor of an insured in a coverage dispute under a crime insurance policy for loss resulting from an email spoofing incident is *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016). In that case, a Georgia district court found the policy's "Computer and Funds Transfer Fraud" language to be ambiguous and construed it in the light most favorable to the insured to provide coverage. In doing so, the court relied on the Texas district court's decision in *Apache Corp. v. Great Am. Ins. Co.*, 2015 WL 7709584 (S.D. Texas Aug. 7, 2015), which was a decision that was reversed by the Fifth Circuit Court of Appeals (as discussed herein) after the *Principle Solutions* decision was issued. The *Principle Solutions* decision has been appealed to the Eleventh Circuit Court of Appeals, which has not yet decided the appeal.

[4] On appeal, the court also rejected the insured's contention that the policy's Forgery provision — which provided that the insurer "shall pay . . . for direct loss sustained by an Insured resulting from Forgery or alteration of a Financial Instrument committed by a Third Party" — applied to forged emails, holding that the phrase "of a Financial Instrument" modified both "Forgery" and "alteration" and that "under a natural reading of the policy, forgery coverage only extends over the forgery of a financial instrument." Additionally, the court held that the loss was not covered under the policy's Funds Transfer Fraud provision — which covered loss resulting from "fraudulent . . . instructions issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from an account maintained by an Insured Organization at such Institution without an Insured Organization's knowledge or consent" — since the insured requested and knew about the wire transfers and since the insured's receipt of the emails did not trigger coverage because the insured was not a financial institution. *Id.* at 628-629.

related professionals

H. Thomas Davis, Jr. / Partner

D 212-238-8850

davis@clm.com

John M. Griem, Jr. / Partner

D 212-238-8659

griem@clm.com