THOMSON REUTERS
Westlaw®

Insurance coverage for social engineering fraud

By Ken Kronstadt, Esq., *Kelley Drye & Warren*

JANUARY 26, 2018

Social engineering fraud occurs when a scammer tricks a company employee into transferring funds, often by sending an email impersonating a vendor, client or executive of the targeted company. In these increasingly common schemes, the email says the vendor or client's banking information has changed or that the company must immediately wire funds "at the executive's direction."

The emails appear to be authentic because they duplicate the targeted company's logo, look and feel. As part of the scammers' effort to escape detection, they also often use an email domain that differs only slightly from the legitimate domain they are attempting to disguise.

Due to these or similar techniques, target companies have sustained millions of dollars in losses when unsuspecting employees unwittingly comply with the instructions.

Companies seeking coverage for social engineering fraud most often look to their crime/fidelity policy. Insurers often take the position that the loss did not result from a "direct" fraud, saying the loss was caused by the company's intervening actions.

While recent court decisions have been mixed, the overall trend has favored insurers. Given this trend and its impact on a company's bottom line, savvy companies should carefully review their traditional crime/fidelity policies and the increasingly prevalent cyberrisk/liability policies to ensure coverage for loss from social engineering fraud.

Apache Corp. v. Great American Insurance Co.

In an October 2016 opinion that insurers often cite in lawsuits related to social engineering fraud, the 5th U.S. Circuit Court of Appeals denied coverage to Apache Corp. for $1.5 million in losses sustained after company employees routed vendor payments to a phony bank account.[1]

A person identifying herself as an employee of Petrofac, an Apache vendor, called and instructed Apache to change its bank account information for payments to Petrofac. An Apache employee stated that the company would need a formal request on Petrofac letterhead.

A week later, Apache's accounts payable department received an email from a petrofacltf.com domain (the real domain was petrofac.com) instructing them to use a new bank account for future payments. A signed letter on Petrofac letterhead with similar instructions was attached to the email.

An Apache employee called the number on the letterhead to verify the request, and a different Apache employee approved and implemented the change.

A week later, Apache transferred funds to the new bank account for payment of Petrofac invoices. Within a month, Petrofac notified Apache that it had not received nearly $7 million that was due.

Apache submitted a claim to Great American, which had issued it a commercial crime policy.

Social engineering fraud occurs when a scammer tricks a company employee into transferring funds, often by sending an email impersonating a vendor, client or executive of the targeted company.

The policy's computer fraud provision stated that Great American "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 ... to a person ... outside those premises" or "to a place outside those premises."

The trial court ruled in Apache's favor, but the 5th Circuit reversed.

Focusing on the fact that the computer fraud provision required that loss result "directly" from the use of a computer to cause a fraudulent transfer, the court stressed that the computer fraud provision was not intended to reach every fraudulent scheme in which an email communication was part of the process.

The court noted that the fraudulent email was merely incidental to the occurrence of the authorized transfer of money, since the fraudulent transfer occurred "only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it."

Medidata Solutions v. Federal Insurance Co.

Last July a New York federal judge held that Medidata Solutions Inc. was entitled to coverage after company employees were duped into wiring money overseas by an imposter posing as the company's president via email.[2]

An accounts payable employee, Alicia Evans, received an email purportedly sent from Medidata's president, bearing his name,

email address and picture. The message said the company was finalizing an acquisition, that an attorney named Michael Meyer would contact Evans, and that she should devote her full attention to his demands.

Later that day, Evans received a phone call from "Meyer," demanding that she process a wire transfer. Evans explained she would need an email from Medidata's president requesting the wire transfer and approval from Medidata's vice president, Ho Chin, and director of revenue, Josh Schwartz.

Chin, Evans and Schwartz then received an email purportedly sent by Medidata's president instructing Evans to complete the wire transfer.

Evans then initiated the transfer, which Schwartz and Chin approved. Nearly $4.8 million was wired to the bank account provided by Meyer and, two days later, Meyer requested a second wire transfer.

Thinking that the email address in the "reply to" field seemed suspicious, Chin spoke to Evans, who sent an email to Medidata's president inquiring about the wire transfers. The president said he had not requested the transfers and the employees then realized the company had been defrauded.

Medidata submitted a claim to Chubb Ltd., which had issued the company a crime policy.

Finding the 5th Circuit's decision in *Apache* unpersuasive, the District Court ruled in favor of Medidata under two separate policy provisions.

First, it deemed the loss covered under the computer fraud coverage provision, which protected against the "direct loss of money, securities or property sustained by an organization resulting from computer fraud committed by a third party."

The court concluded that, while Medidata's computers were not directly hacked by a third party, the requirements of the provision were still met because the thief gained entry into Medidata's email system with spoofed emails.

These emails were also armed with a computer code that masked his true identity and made the emails appear as though they originated from Medidata's president.

The court also deemed the loss covered under the policy's funds transfer fraud coverage provision, which protected against "direct loss of money or securities sustained by an organization resulting from funds transfer fraud committed by a third party."

Chubb had argued that the wire transfer was voluntary and made with Medidata's knowledge and consent.

The court rejected this argument, stating that "the fact that [Evans] willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction" or a voluntary one. "Larceny by trick is still larceny," it said.

American Tooling Center v. Travelers Casualty & Surety Co.

Relying in part on *Apache*, a Michigan federal court ruled in August 2017 that Travelers Casualty & Surety Co. was not obligated to cover American Tooling Center Inc.'s losses resulting from a fraudulent, email-based scheme.[3]

American Tooling outsourced some of its work to manufacturing companies overseas, one of which was YiFeng Automotive Die Manufacture Co. American Tooling Vice President/Treasurer Gary Gizinski sent an email to his contact at YiFeng, requesting copies of all outstanding emails.

Gizinski received a response from a scammer using the domain "yifeng-rnould," which is easily confused with the correct domain,"yifeng-mould.com." The scammer instructed American Tooling Center to send payment for several invoices to a new bank account.

Without verifying the new banking instructions, American Tooling wired $800,000 to a bank account not controlled by YiFeng. After the fraud was discovered, the money could not be recovered.

American Tooling sought coverage for the loss from Travelers, which issued American Tooling a policy covering "computer crime," in which Travelers would pay American Tooling for its "direct loss of, or direct loss from damage to, money, securities and other property directly caused by computer fraud." The court held that the fraudulent emails did not "directly" or "immediately" cause American Tooling to transfer funds from its bank account.

Rather, the court found that American Tooling took several steps between when it received the fraudster's emails and when it transferred the funds, such as verifying production milestones, authorizing the transfers and initiating the transfers without verifying bank account information. As a result, the court could not find a loss "directly caused" by the use of any computer.

Principle Solutions Group v. Ironshore Indemnity

Less than a year before *Medidata*, a Georgia federal court found that Ironshore Indemnity Co. was required to cover a $1.7 million loss from a transfer resulting from a fraudulent scheme similar to that in *Medidata*.[4]

In the case, Principle Solutions Group's controller received an email from a person purporting to be Josh Nazarian, one of the company's managing directors. The email referenced a company acquisition and instructed the controller to "treat the matter with the utmost discretion" and to work with an attorney, Mark Leach, to ensure that the wire went out that day.

Later that morning, the controller received an email from a "Mark Leach," who represented himself as a partner at Alston & Bird. The email said "Leach" was reaching out at Nazarian's request, and it included instructions for wiring the funds to a bank in China.

The controller approved the wire transfer after Leach called the controller to stress that they needed to complete the transaction that day. The financial institution's fraud prevention unit called the controller for verification and, after being told that Leach had verbally received the wire instructions from Nazarian, released the transfer.

When the controller spoke with Nazarian the next day, the pair realized the company had been defrauded. Nazarian immediately called the financial institution's fraud department, but the company could not recover the $1.7 million.

Principle sought coverage from Ironshore, which had issued a commercial crime policy providing "computer and funds transfer fraud" coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer, pay or deliver 'money' or 'securities' from that account."

Ironshore argued that the loss did not result "directly" from a fraudulent instruction because Leach conveyed additional information for the wire transfer after the initial email and Principle's employees set up and approved the transfer.

The court found the policy language was ambiguous, either requiring an immediate link between the injury and its cause, as Ironshore contended, or providing coverage even if there were intervening events between the fraud and the loss.

As courts commonly do when deeming policy language ambiguous, the court construed the policy in the light most favorable to the insured and found for Principle.

Notably, in its August 2016 opinion, the *Principle Solutions* court relied on the *Apache* trial court opinion to support its positon. As discussed above, however, the 5th Circuit reversed that trial court opinion in October 2016, less than two months after *Principle Solutions* was decided.

Pestmaster Services v. Travelers Casualty & Surety Co.

In a case involving computer fraud coverage but not social engineering fraud, the 9th U.S. Circuit Court of Appeals held that there was no coverage for a fraudulent scheme resulting in losses that did not flow "immediately" and "directly" from the use of a computer.[5]

In *Pestmaster*, a payroll contractor of the insured, Priority 1 Resource Group, was hired to withhold and submit payments for the insured's payroll taxes. Priority 1 prepared invoices for Pestmaster Services Inc. and was authorized to initiate transfers of funds from Pestmaster's bank account to Priority 1's bank account to pay invoices approved by the insured.

Instead of paying the approved invoices, Priority 1 fraudulently used Pestmaster's funds to pay Priority 1's own expenses, leaving Pestmaster indebted to the IRS for payroll taxes.

After Travelers denied coverage, Pestmaster brought suit against the insurer, which had issued a "crime plus wrap" policy to Pestmaster that included, in pertinent part, a computer crime insuring agreement covering "direct loss of, or your direct loss from damage to, money, securities and other property directly caused by 'computer fraud.'"

The District Court sided with Travelers, finding the "claimed losses did not 'flow immediately' and 'directly' from Priority 1's use of a computer" because they did not occur until after the transfer, when Priority 1 used the funds to pay its own obligations rather than Pestmaster's federal payroll taxes.[6]

The 9th Circuit affirmed, reasoning that the phrase "fraudulently cause a transfer" required an unauthorized transfer of funds, and no such unauthorized transfer occurred because Pestmaster authorized the transfer to Priority 1.

"Because computers are used in almost every business transaction," the court wrote, "reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this crime policy into a 'general fraud' policy," essentially covering losses from all forms of fraud rather than a specified risk category.

Several other notable cases have similarly denied coverage outside the context of social engineering fraud where a company was victimized through the incidental, rather than direct, use of a computer.

For example, courts have held in the insurers' favor where users exploited a loophole in a prepaid debit card authorization process using a telephone to redeem funds, resulting in a behind-the-scenes interaction with a computer and causing losses of over $10 million.

They have also denied coverage where a company offering health insurance to Medicare-eligible individuals sustained losses of over $18 million for payment of fraudulent claims for medical services that were falsely entered into a computer system as having been performed.[7]

SECURING COVERAGE

Whether a company is able to obtain coverage for social engineering fraud under a crime/fidelity policy will depend largely on the precise language of the company's policy. Even a slight variance in policy language can have a dramatic impact on coverage.

As the cases discussed above illustrate, even where a crime/fidelity policy requires that loss be caused "directly" by fraud, courts have reached inconsistent conclusions on the coverage question. It is possible, as in *Medidata* and *Principle Solutions,* that a court will afford coverage even when intervening acts separate the fraudulent conduct and the loss sustained.

A company looking to ensure coverage should not assume that a court will rule in its favor on these issues. As of now no cases have relied on *Medidata*'s holding to find coverage, and two cases have declined to follow *Medidata*.[8]

As discussed above, *Principle Solutions* relied in large part on the trial court ruling in *Apache*, which was reversed less

than two months after the *Principle Solutions* court issued its opinion.

More cases have denied than granted coverage for social engineering fraud where the crime/fidelity policy required that the loss be caused "directly" by fraud. These decisions reasoned that intervening actions between the fraud and the loss negated coverage.

Given the increasing demand to insure against social engineering fraud risks, some insurers have begun to offer policy endorsements specifically providing coverage for these claims.

Policyholders should scrutinize the language of these endorsements. They may be subject to a sublimit; they may cover some, but not all social engineering fraud risks; and they may be subject to additional exclusions.

Companies seeking coverage for social engineering fraud claims may also wish to consider a cyberliability insurance policy. Although these policies are often more specifically tailored to cover data breaches and similar events, there is no "standard" cyberliability insurance form, and the types of coverages available often differ drastically from insurer to insurer.

Many cyberliability policies exclude "voluntary parting" or "voluntary payments," that is, losses flowing from the insured's voluntary transfer of money to a third party. Though these exclusions would bar coverage where an employee is tricked into wiring money, savvy companies can specifically request coverage for social engineering fraud for only a nominal additional premium.

CONCLUSION

Simply obtaining a crime/fidelity or cyberliability policy does not ensure coverage if a company falls prey to social engineering fraud. The specific language used in a company's individual policy will always determine coverage.

As the cases above illustrate, where a crime/fidelity policy requires "direct" causation — as many often do — it appears somewhat more likely that a court will deny coverage for social engineering fraud where there are intervening actions between the fraud and the loss sustained. In light of *Medidata*'s holding, however, policyholders have legitimate grounds to argue for coverage.

Given the significant differences in the policy forms issued across the cyberliability market, even where social engineering fraud fits within the coverage grant under some policies, a "voluntary parting" or "voluntary payments" exclusion may preclude coverage.

Because courts have yet to address coverage for social engineering fraud under cyberliability policies, and given the lack of uniformity in policy language, it is difficult to predict how a court will decide coverage.

In the face of this uncertainty, policyholders should get an endorsement specifically designed to provide social engineering fraud coverage under either a crime/fidelity or cyberrisk policy.

Because these types of endorsements are so new however, policyholders need to carefully scrutinize their wording to make sure they cover the types of social engineering fraud risks the company may face.

NOTES

[1] *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. App'x 252 (5th Cir. 2016).

[2] *Medidata Solutions Inc. v. Fed. Ins. Co.*, No. 15-cv-907, 2017 WL 3268529 (S.D.N.Y. July 21, 2017).

[3] *Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-cv-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

[4] *Principle Solutions Grp. LLC v. Ironshore Indem.*, No. 15-cv-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).

[5] *Pestmaster Servs. v. Travelers Cas. & Sur. Co. of Am.*, 656 Fed. App'x 332 (9th Cir. 2016).

[6] *Pestmaster Servs. v. Travelers Cas. & Sur. Co. of Am.*, No. 13-cv-5039, 2014 WL 3844627 (C.D. Cal. July 17, 2014).

[7] *InComm Holdings Inc. v. Great Am. Ins. Co.*, No. 15-cv-2671, 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017); *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 37 N.E.3d 78 (N.Y. 2015).

[8] *See Am. Tooling*, 2017 WL 3263356; *Posco Daewoo Am. Corp. v. Allnex USA Inc.*, No. 17-cv-483, 2017 WL 4922014 (D.N.J. Oct. 31, 2017).

This article first appeared in the January 26, 2018, edition of Westlaw Journal Insurance Coverage.

ABOUT THE AUTHOR

Ken Kronstadt is a senior associate at **Kelley Drye & Warren** in Los Angeles, where he is a member of the firm's insurance recovery group. He concentrates his practice in the areas of insurance coverage litigation and counseling in the construction and entertainment industries, and he has in-depth knowledge of insurance coverage for emerging cybersecurity and data privacy-related events.