wiley

ARTICLE

Covering New Fraud Risks With Traditional Policies

Law 360
May 25, 2017

A typical social engineering or fraudulent wire instruction scam is painfully simple – and often successful. In one common scenario, a fraudster researches a company, mimics an employee's (often a high-ranking officer) email address and sends a wire transfer request to the accounting department, often indicating that the request is time-sensitive and top secret. The target, feeling pressure from this faux-CEO, wires the money to the fraudster's account. By the time the scam is discovered, the money and fraudster are long gone.[1]

Targets of such attacks have found that whether insurance coverage is available for fraudulent transfer scams is highly dependent on the precise language of their specific policies. While a small number of courts have held that certain policies provided coverage for a fraudulent instruction loss, as a general rule, these losses present relatively new exposures that do not tend to fit neatly into any traditional forms of coverage. This fact has led several insurers to introduce policies or endorsements tailored specifically to business email compromise and fraudulent instruction scams.

In this article, we analyze the coverage issues likely to arise, and the policy provisions likely to be determinative, when an insured seeks coverage for a fraudulent instruction loss under various types of insurance policies. We analyze crime and fidelity policies, financial institution bonds and cyber or data breach policies, among others. The results are highly dependent on the insured's specific policy language, as well as the circumstances of the underlying loss. Overall, however, the cases that have been litigated to date show that, more often than not, traditional policies do not cover these new exposures.

Authors

Mary E. Borja
Partner
202.719.4252
mborja@wiley.law

Edward R. Brown
Partner
202.719.7580
erbrown@wiley.law

Practice Areas

Commercial Crime Insurance and Fidelity Bonds

Cyber Insurance

General Liability

Insurance

Crime Coverage

The first coverage an insured may look to after a fraudulent wire instruction loss is its first-party crime policy. Though nonstandard, commercial crime policies typically provide coverage for employee theft, forgery and alteration, burglary and robbery, counterfeit money, and computer crime or computer fraud. Some will also cover theft of a client's property or theft of securities. Because a fraudulent wire instruction loss involves theft and, in a general sense, computer crime, an insured often will tender such a claim under its crime policy.

While some commercial crime loss insurers have added insuring agreements or endorsements to address fraudulent instruction losses, the typical commercial crime policy has not evolved to cover this new risk. Forgery insuring agreements generally require a forged financial instrument, and computer fraud insuring agreements generally require intrusion into the insured's computer networks – neither of which are involved in the typical fraudulent instruction scheme. These losses also do not usually involve employee dishonesty. Though some commercial crime policies may include fraudulent transfer insuring agreements, these tend to provide tailored rather than blanket coverage. Two federal appeals courts have recently analyzed coverage for a fraudulent wire instruction loss under several crime policy insuring agreements and held that the policies did not afford coverage for this type of loss.

Most recently, in *Taylor & Lieberman v. Federal Insurance Co.*, the U.S. Court of Appeals for the Ninth Circuit affirmed a district court's conclusion that a commercial crime policy issued to an accounting firm did not cover a fraudulent wire instruction claim. No. 15-56102 (9th Cir. Mar. 9, 2017). The insured accounting firm in that case had received wire instructions from a client's email account (sent by an unauthorized third party that had gained access to the email account), and directed the client's bank to transfer the funds. The appeals court analyzed whether the policy's insuring agreement – providing coverage for direct loss "resulting from Forgery or alteration of a Financial Instrument by a Third Party" – applied to forged emails. The policyholder contended that the phrase "of a Financial Instrument" modified only "alteration," such that any forgery, including a forged email, triggered coverage. The court disagreed, holding that, "under a natural reading of the policy, forgery coverage only extends over the forgery of a financial instrument."

The appeals court also determined that the policy's computer fraud coverage and funds transfer fraud coverage parts likewise did not cover the loss. The computer fraud coverage part required "unauthorized entry" into the insured's computer systems. The court concluded that the mere sending of emails into the insured's network did not constitute "entry," nor were those emails an unauthorized "introduction of instructions" that "propagate[d]" themselves through the insured's computer system, as the policyholder contended.

Finally, the *Taylor & Lieberman* court held that the claim did not fit within the funds transfer fraud coverage part. That coverage part afforded coverage for loss arising from fraudulent instructions "issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by an Insured Organization, without an Insured Organization's knowledge or consent." The insured had received fraudulent emails, then directed its client's bank to wire the funds as instructed. The court concluded that neither the receipt of the emails nor the direction to the bank satisfied the policy language. Because the

insured knew about and requested the wire transfers by the bank, the transfers were not "without an Insured Organization's knowledge," and therefore were not covered. In addition, the insured's receipt of the emails did not trigger coverage because the insured was not a financial institution. As a result, the court held that the policy did not afford coverage for the loss.

The Fifth Circuit also recently held that a commercial crime policy's computer fraud insuring agreement did not apply to a fraudulent instruction loss. In *Apache Corp. v. Great American Insurance Co.*, the Fifth Circuit analyzed whether a business email compromise loss resulted "directly from the use of any computer to fraudulently cause a transfer." No. 15-20499 (5th Cir. Oct. 18, 2016). The policy covered, in relevant part, "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." The insurer denied coverage because the insured's "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds." The district court had granted summary judgment in favor of the insured after ruling that the fraudulent email was a "substantial factor" in the scheme. In so doing, the court rejected the argument that coverage under the policy was limited to losses caused by computer hacking.

On appeal, the Fifth Circuit reversed the decision and rendered judgment for the insurer. The court recognized a "cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly [caused] by the computer use," and it found that authority persuasive. The court determined that the "computer use" at issue "was an email with instructions to change a vendor's payment information." While the Fifth Circuit acknowledged that the use of "email was part of the scheme[,] ... the email was merely incidental to the occurrence of the authorized transfer of money." The court further noted 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." The court therefore ruled that the business email compromise loss caused through social engineering did not "result[] directly from the use of any computer to fraudulently cause a transfer."

While the *Apache* appeal was pending, a Georgia federal district court, relying in part on the *Apache* district court's holding, held that a business email compromise loss was covered by a commercial crime policy because it resulted directly from a fraudulent instruction. *Principle Solutions Grp. LLC v. Ironshore Indem. Inc.*, Civil Action No. 1:15-CV-4130-RWS (N.D. Ga. Aug. 30, 2016). The policy at issue provided 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." The insurer denied coverage because it determined that the loss did not result "directly" from the instruction, because there were several intervening steps between the instruction and the loss, including the insured's employee obtaining additional information for the wire and setting up and approving the wire transfer. The court determined that the provision was ambiguous and construed it in favor of the insured. In the court's view, the policy could be interpreted to provide coverage only for losses with an immediate link to the fraudulent instruction, or it could be interpreted to also cover losses with intervening events between the fraud and the loss. The insurer moved for reconsideration in light of the Fifth Circuit's decision in *Apache* reversing the district court opinion, but the Principle Solutions district court denied the motion, distinguishing both the *Apache* and *Taylor & Lieberman*

appellate court decisions. The insurer has appealed.

More recently, another Georgia federal district court held – relying in part on the Fifth Circuit's *Apache* decision – that a loss from a fraudulent scheme using telephones to exploit a computer coding vulnerability did not "directly" result from computer fraud and was not caused by "use[] of a computer," although the insured's computers involved in the transaction. *InComm Holdings Inc. v. Great Am. Insurance Co.*, 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017). Although this case did not involve a fraudulent wire instruction loss, the court's reasoning that losses involving a computer at any point in the causal chain do not necessarily constitute "computer fraud" is instructive.

As shown in *Apache* and *Principle Solutions*, coverage for these losses often turns on questions of causation. For example, in a recent federal district court case, the key issue was whether the loss resulted directly or indirectly from the entry of data into a spreadsheet. In *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*, a Washington federal district court determined that a fraudulent instruction loss was barred from coverage by a crime policy exclusion for "loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System" unless otherwise covered under certain insuring agreements that clearly did not cover this loss. No. C14-1368RS (W.D. Wash. July 8, 2016). The insured acknowledged that its employee was an authorized user and input electronic data into its computer system by adding the new wire information to a spreadsheet to track payment details. The insured argued, however, that the loss did not result directly or indirectly from this data entry, but instead from the employee's entry of the data into the computer system of a third party, the bank. The court disagreed.

The court concluded that, although entering the data into a third-party computer system may have been the final step that led to the loss, the necessary step prior to the transfer involved entering data into the insured's own computer system. The court therefore held that, based on the plain language of the exclusion, there was no coverage. Because the exclusion barred coverage entirely, the court did not reach the question of whether the loss triggered the crime policy's insuring agreement in the first instance.

Financial Institution Bond Coverage

A second type of coverage that has been the subject of litigation with respect to business email compromise losses is coverage under financial institution (FI) bonds issued to banks and other financial institutions. These bonds generally cover employee dishonesty, burglary, robbery, counterfeiting, forgery and certain types of money and securities fraud. Fraudulent instruction coverage may be available to an insured under FI bonds, but generally only where certain defined conditions, often involving the bondholder's procedures and authorizations for transfers, are met. For instance, in *Universal City Studios Credit Union v. Cumis Insurance Society*, the bond provided coverage if the credit union used "a commercially reasonable security procedure set forth in a written funds transfer agreement, signed by the member or the member's authorized representative, that governs the transaction and instruction." 145 Cal. Rptr. 3d 650 (Ct. App. 2012). In that case, the credit union's loss was not covered because the funds transfer agreement governing the transaction provided that the transfer request must be signed by the customer's authorized representative. Because the signature on the request form was forged, rather than signed by an authorized representative, the transfer did

not satisfy the security procedures set forth in the signed agreement, and as a result, the FI bond did not cover the loss.

The Ninth Circuit reached a similar result in *First National Bank of Northern California v. St. Paul Mercury Insurance Co.*, 603 Fed. Appx. 597 (9th Cir. 2015). In that case, the bond limited coverage to transfers for "customers," defined to mean individuals or entities that had a written agreement with the bank to rely on wire transfer instructions communicated by phone or fax. The court found that the creators of the trust from which funds were wired were not "customers" because they had no such written agreement. The bondholder argued that a signature card, account agreement, and the bank's security procedures combined constituted the required written agreement. The court found otherwise, holding that the district court correctly concluded that the bank's transfer of funds from the trust was not a covered loss.

A Pennsylvania federal district court reached the same conclusion in *Sb1 Federal Credit Union v. FinSecure LLC*, because the bondholder had failed to allege that the customer agreements were written, that those agreements included a funds transfer agreement that addressed the transactions at issue, or that they were signed by the account holder – all of which the bond required. 14 F. Supp. 3d 651 (E.D. Pa. 2014). The bondholder also sought coverage under the bond's forgery and employee dishonesty coverages. The *Sb1* court determined that the employee dishonesty coverage did not apply because there was no evidence that the employee who authorized the transfer had the intent to harm the credit union or obtain a financial benefit, and an exclusion for "loss resulting directly or indirectly from a fraudulent instruction through E-mail, Telefacsimile or Telephonic means" precluded coverage under the forgery coverage part.

Two courts have held that similar losses were covered under financial institution bonds, but neither case appears to set a strong precedent for this type of coverage. In *Bank of Ann Arbor v. Everest National Insurance Co.*, the Sixth Circuit affirmed a district court's conclusion that a bond's "loan loss" exclusion did not preclude coverage because the loss from the wire was not an extension of credit and because the loss did not result from the nonpayment of a loan. 563 Fed. Appx. 473 (6th Cir. 2014). The court did not reach the insurer's argument that the bond covered losses resulting from reliance on a forged wire transfer only if the bondholder had actual physical possession of the original instrument on which the forgery appeared, because the insurer was found to have waived that argument. Because of the waiver, this case offers little precedential value on the substance of the coverage issues.

The second such case did not involve waiver, but involved fraudulent instructions sent via fax. *Missouri Bank & Trust Co. of Kansas City v. OneBeacon Insurance Co.*, 688 F.3d 943 (8th Cir. 2012). The policy at issue included an insuring agreement providing that:

[l]oss resulting directly from ... transferring ... any funds ... on the faith of any Written instructions or advices directed to [Missouri Bank] and authorizing or acknowledging the transfer ..., which instructions or advices purport to have been signed or endorsed by any customer of [Missouri Bank] ..., but which instructions or advices either bear a signature which is a Forgery or have been altered without the knowledge and consent of such customer or banking institution ...

The insurer had determined that the fax was not "Written" but instead was an electronic record, as the policy specified that electronic records were not "Writings." The court concluded, however, that a fax was a "Writing" / "Written" because it had been intentionally reduced to tangible form, and the bond therefore covered the transfer. While this case is instructive in the context of faxed instructions and this particular policy language, because of those nuanced facts, its reasoning likely would not extend to the typical fraudulent instruction scenario involving email.

Cyber or Data Breach Coverage

Because business email compromise losses are technology-related, an insured may also submit these losses to their cyberloss insurer for coverage. Though coverage will depend on the actual language of each policy, cyberpolicies will typically cover business email compromises only if they include an endorsement or insuring agreement tailored specifically to fraudulent instruction.

Coverage for a fraudulent wire transfer under a cyberpolicy does not appear to have been litigated, but analysis of cyberpolicies shows that these risks often will not trigger any insuring agreement. Cyber or data breach coverage typically requires one of the following: unauthorized access or intrusion into the insured's computer system or the insured's failure to prevent a breach of its computer networks; the unauthorized use, disclosure or loss of information or data within the insured's custody or control; or the duty to notify individuals of unauthorized access to or use of their data under applicable breach notification laws.

The traditional fraudulent wire transfer scheme is not likely to constitute any of these triggering incidents. Rather than breaching the insured's computer systems, the fraudulent third party simply hoodwinks the insured's agents by using an email address that is similar to that of an authorized agent. Even where the third party spoofs an email header to make it appear that it has come from the chief financial officer's or CEO's actual email address, these acts do not require or typically involve unauthorized access to the insured's computer systems. The cases analyzing coverage under computer fraud insuring agreements in crime policies, such as *Taylor & Lieberman* and *Apache*, are informative here. The courts in those cases concluded that sending an email to the insured and convincing the insured to follow fraudulent instructions does not involve intrusion into the insured's computer system. Presumably, a court conducting this inquiry under a cyber policy would reach the same conclusion.

Nor do fraudulent instruction losses involve disclosing any data to the anonymous third party. In other words, fraudulent instruction losses do not constitute disclosure or loss of information or data within an insured's custody, and as a result, they do not trigger the insured's duties under breach notification laws. Moreover, cyberpolicies often provide that, to implicate coverage, the type of data compromised must be private health information, financial information or other sensitive or personal information. Typically, fraudulent wire schemes do not involve the compromise of any of the above; the only data transmitted is the wiring information for the fraudster's account. In light of these standard policy provisions, cyber policies are unlikely to respond unless they include an insuring agreement specific to fraudulent instruction losses.

Other Coverages

When pursuing coverage under other types of policies, such as first-party property or errors and omissions liability policies, a fraudulent instruction loss will rarely, if ever, trigger any insuring agreement and may also be precluded by certain exclusions. For example, an insured sought coverage for a fraudulent instruction loss under a businessowners property policy in *Schmidt v. Travelers Indemnity Co. of America*, 101 F. Supp. 3d 768 (S.D. Ohio 2015). The court in Schmidt held that the loss was not covered due to a "voluntary parting" exclusion, because the loss was not a suspension of business, and the cashier's checks involved in the transfer were not "business personal property."

These claims likewise may be outside the scope of most errors and omissions policies if transferring of funds is not part of the insured's "professional services" and thus falls outside the insuring agreement. An architecture firm, for instance, may have a hard time arguing that was rendering its professional services in completing a wire transfer. In addition, these policies require a third-party claim, and a loss to the insured's own accounts would generally not give rise to a claim by any third party. Relatedly, these policies generally require that the insured's error or omission take place in rendering its professional services "for others" or "for clients or customers." Where the target of social engineering attacks wires funds from its own accounts to the fraudulent third party, the wiring was usually not done "for others."

E&O coverage may be a closer call where the insured's professional services do involve managing accounts for its clients — for instance, an accounting firm or real estate management firm. In these instances, whether the insuring agreement is triggered will be a fact-specific inquiry based on the type of professional services the insured renders and the transaction in question. Still, even if the transaction triggers the insuring agreement, certain exclusions may preclude coverage. For instance, many E&O policies exclude coverage for claims arising from the commingling, misappropriation, improper use or conversion of funds. While in some policies these exclusions are limited to commingling, misappropriation, improper use or conversion of funds by the insured (in which case they may not bar coverage for a fraudulent instruction loss), many policies contain no such limitation. In those cases, the fraudulent third party's misappropriation or conversion of the funds may implicate the exclusion. See, e.g., *Accounting Res. Inc. v. Hiscox Inc.*, No. 3:15-ccv-01764 (D. Conn. Sept. 30, 2016).

Conclusion

Because business email compromise losses are relatively novel, policies that afford coverage for these losses tend to be the exception, rather than the rule. It should come as no surprise that the market has responded and a number of carriers now offer policies or endorsements specifically tailored to respond to these losses. If an insured wants coverage for this risk, its best bet is to request a policy, endorsement or insuring agreement tailored to cover fraudulent instruction and social engineering losses.

---

[1] A fraudster may target a company and mimic an officer's email address when the fraudster knows that officer is scheduled to be difficult to reach.