An Evolving Landscape: Insurance Coverage for Social Engineering Wire-Fraud Scams

By Jessica H. Park and John G. O'Neill


A company employee receives an email from a trusted vendor that instructs the employee to update the bank account information used to pay the vendor. The employee complies, wiring vendor payments to the new account—only to discover soon after that the "new" bank account really belongs to a very clever cybercriminal. Thousands or even millions of dollars wired to the new account have been lost, with no viable means of recovery.

The company turns to its crime insurance policy, which insures against certain types of losses involving "computer fraud," among others. But will it provide coverage for this loss? What are the coverage issues that may come into play?

This article will analyze the anatomy of a social engineering scheme and the potential coverage arguments and defenses that may be implicated by wire-fraud claims.

Anatomy of a Social Engineering Scam

Social engineering is a type of fraud in which a perpetrator, often via email, attempts to exploit the victim's natural social and interpersonal tendencies to commit a theft or other crime. This may take the form of a spear-phishing attempt in which a cybercriminal targets a particular person in an effort to trick him or her into sending the criminal funds or information. Variations on the potential scenarios are virtually endless, but the end result is the same: a substantial sum of money is wired to a cybercriminal's bank account, and once the funds have been wired, they usually cannot be retrieved.

Social engineering fraud has become both more costly and more sophisticated over time. In 2017, the FBI warned that this type of "business e-mail compromise," or "BEC," scam had continued to "grow, evolve, and target businesses of all sizes," and reported a 1,300 percent increase in identified BEC losses over a two-year period. *Business E-Mail Compromise, Cyber-Enabled Financial Fraud on the Rise Globally*, FBI News (Feb. 27, 2017), https://www.fbi.gov/.

Such scams can be quite elaborate, with the potential to trick even careful and vigilant employees. A 2017 New York federal court case, *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F. Supp. 3d 471 (S.D. NY 2017), *affirmed*, 2018 WL 3339245 (2d Cir. 2018), provides a prime example. In that case, a cloud-services provider, Medidata, was the victim of a fraudulent wire transfer. The company learned that fraudsters had manipulated the Google Gmail platform that the company used for its emails by embedding a code into spoofed messages, tricking the Gmail platform into recognizing the emails as intracompany communications. This caused the platform to populate the messages with the company president's information, rather than that of the true sender. The result was an authentic-looking communication, which, when paired with the thieves' multi-layered approach and the fact that the company really was considering an acquisition, achieved the fraudsters' desired result. The company was able to obtain coverage for its loss; some others, however, have not fared as well.

> Claims under such computer fraud provisions have given rise to a variety of coverage disputes when thieves trick authorized users into effectuating transfers.

Potential Coverage Sources

In wire-fraud losses, policyholders have sought coverage under several provisions of such policies, including those addressing "computer fraud," "funds transfer fraud," and in some cases, "forgery and alteration."

Coverage Under Computer Fraud Provisions

"Computer fraud" provisions typically cover loss of securities, money, or property resulting from some form

of computer-related, fraudulent transfer. For example, such a provision might provide coverage for "loss of… securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property[.]" Another, somewhat more detailed, variant might provide coverage for loss resulting from a fraudulent "entry" or "change" of data in a computer system. Claims under such computer fraud provisions have given rise to a variety of coverage disputes when thieves trick authorized users into effectuating transfers.

The courts have reached different conclusions in their analyses of coverage. In the Fifth Circuit decision, *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252, 254 (5th Cir. 2016), Apache sought coverage under the computer fraud provision of its crime policy, which covered loss "resulting directly from the use of any computer to fraudulently cause a transfer[.]" The Fifth Circuit held that there was no coverage and concluded that the fraudulent transfer was the result of intervening events and not caused "directly" by computer use. *Id.* at 252.

However, the Sixth Circuit has reached a different analysis. In *American Tooling Center v. Travelers Cas. & Sur. Co. of America*, 2018 WL 3404708 (6th Cir. July 13, 2018), the Sixth Circuit addressed whether there was coverage when fraudulent emails instructed the insured to change the bank account information for payments owed to the vendor, and the insured complied, unwittingly wiring payments for legitimate vendor invoices to the perpetrators' bank account. The Sixth Circuit held that there was nothing in the policy's computer fraud language that expressly required hacking or unauthorized access.

Coverage Under "Funds Transfer Fraud" Provisions

"Funds transfer fraud" provisions are intended to provide coverage for unauthorized transfers from an insured's bank account, but typically they require the transfer to have resulted from a fraudulent instruction issued without the insured's knowledge or consent. Of course, the fraud in a social engineering scheme involves deceiving the insured into issuing an erroneous transfer instruction to its own bank, so the instruction is almost certain to be something that an employee of the insured is aware of and has authorized. Although decisions construing funds transfer fraud provisions in other contexts have often found no coverage when the transfer instruction was authorized by the insured, even if it was associated in some way with fraud, decisions involving social engineering losses are less uniform, as will be discussed below.

Although decisions construing funds transfer fraud provisions in other contexts have often found no coverage when the transfer instruction was authorized by the insured, even if it was associated in some way with fraud, decisions involving social engineering losses are less uniform.

In *Pestmaster Servs. Inc. v. Travelers Cas. and Sur. Co. of America*, the insured, a pest control company, suffered losses due to an outside payroll administration provider's misappropriation of funds that had been transferred from the insured's account to cover payroll tax obligations. *See* 2014 WL 3844627 (C.D. Cal. July 17, 2014), *vacated in part on other grounds*, 656 Fed. Appx. 332 (9th Cir. 2016). The *Pestmaster* court held that the language of the funds transfer insuring agreement was unambiguous, and did not provide coverage for valid electronic transactions, such as the authorized ACH transfers to the payroll administrator, even though the administrator had not used the funds for their intended purpose. The court observed that the coverage was intended to protect against someone impersonating the insured or altering the electronic instructions to divert funds from the rightful recipient. *See id.* at *5 (citing *Northside Bank v. American Cas. Co.*, 60 Pa. D&C 4th 95 (Pa. County Ct. 2001) (further citation omitted)).

Coverage Under "Forgery and Alteration " Provisions

"Forgery and alteration" coverage generally extends to losses caused by forgery or alteration of a financial instrument, such as a check, draft, or promissory note. Insureds that have fallen prey to social engineering fraud have offered several creative arguments in favor of coverage under forgery and alteration provisions; however, courts have uniformly rejected them. For the most part, courts have reasoned that such schemes do not involve a financial instrument, but rather involve a wire transfer, which is legally and factually distinguishable. Courts likewise draw a distinction between the fraudulent instructions that are

central to social engineering schemes and the forgery of a signature upon an instrument necessary to trigger coverage under this type of provision. While policyholders' counsel have offered creative arguments, courts have been unwilling to equate fraudulent emails or wiring instructions with financial instruments, or to otherwise relax this key coverage requirement.

Conclusion

The three crime policy provisions under which insureds are most likely to seek coverage in connection with social engineering wire-fraud losses—"computer fraud," "funds transfer fraud," and "forgery and alteration"—each implicate somewhat unique coverage issues and give rise to a variety of potential arguments and defenses. With the exception of "forgery and alteration" cases, results have not been entirely uniform, and the landscape continues to evolve. It will thus be imperative for practitioners, including counsel for both policyholders and carriers, to stay apprised of developments in this area of the law as it continues to develop and mature.

Jessica H. Park *and* **John G. O'Neill** *are partners with the Boston law firm Sugarman Rogers Barshak & Cohen PC. Ms. Park works with national and regional insurance carriers on insurance-coverage matters, lawsuits involving claims of bad faith, extra-contractual liability, and violations of consumer-protection statutes, and reinsurance disputes. She is a member of the DRI Insurance Law, Cybersecurity and Data Privacy, and Women in the Law Committees. Mr. O'Neill focuses his practice on insurance, business disputes, and professional liability defense. He regularly advises and represents insurers in coverage and bad-faith matters throughout the United States. Mr. O'Neill is a member of the DRI Insurance Law Committee.*