An Evolving Landscape

Insurance Coverage for Social Engineering Wire-Fraud Scams

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

The three crime policy provisions under which insureds are most likely to seek coverage in connection with social engineering wire-fraud losses each implicate somewhat unique and evolving coverage issues.

A company employee receives an email from a trusted vendor, which 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 how courts across the country have grappled with these questions in the face of increasingly sophisticated wire-transfer fraud scams, often accomplished through the use of social engineering ploys. While the results are fact specific and not always uniform, common threads have developed. One key theme is whether the use of an email message to trick a recipient is sufficient to trigger coverage, or whether something more akin to hacking or system intrusion is required. This article will discuss trends that have emerged in this evolving area of the law, and 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 infor-

■ Jessica H. Park and John G. O'Neill are partners with the Boston law firm Sugarman, Rogers, Barshak & Cohen, P.C. 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, as well as 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.

mation. A typical pattern might look similar to the following:

- A fraudster identifies a target, perhaps an employee in a company's accounts payable or finance department.
- The perpetrator comes armed with inside information gained from infiltrating company networks or other channels. For example, he or she may have learned that the company is in the midst of a large transaction, may know who the company's key vendors or clients are, or may have important information about corporate reporting structures or travel schedules.
- The fraudster emails the targeted employee, impersonating a trusted contact such as a vendor or the employee's supervisor. The impersonation might be achieved in a variety of ways. For example, a perpetrator might use a fake email address that differs from the real one in a subtle way, such as a slight misspelling or substituting the number "1" for the letter "l." Or a more advanced spoofing technique might be used, making the fabricated email all but indistinguishable from the real thing.
- The criminal uses this impersonation, his or her inside knowledge, and the victim's natural social responses to convince the target to wire money to the perpetrator's bank account. The criminal might pretend to be a vendor and instruct the employee to change the wiring instructions for vendor payments that the company is already planning to make. Or the criminal might pretend to be the employee's supervisor—perhaps while the supervisor is traveling out of town—and ask the employee to wire money for an urgent transaction that the company must close.

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/. The FBI's 2017 Internet Crime Report, released in May 2018, similarly reported that the FBI has continued to observe a constant evolution of email compromise scams as the perpetrators' approaches become more refined. According to that report, email compromise scams were linked to the highest losses of any crime type reported to the FBI's Internet Crime Complaint Center: in 2017, the FBI received 15,690 email compromise complaints with adjusted losses of over $675 million, far higher than those associated with corporate data breaches, identity theft, or ransomware. *See* FBI Internet Crime Complaint Ctr., *2017 Internet Crime Report* (May 2018), 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 considering a possible business acquisition. The company instructed its finance personnel—including an accounts-payable employee who was responsible for processing certain company expenses—that they should be prepared to assist with significant transactions on an urgent basis. Soon after, the accounts-payable employee received an authentic-looking email that in all respects appeared to be from Medidata's president. The email included the president's name and email address in the "from" field, and even included the president's photo, as was the company's usual practice. The email instructed the employee that Medidata was close to finalizing a highly confidential acquisition, that the employee would be contacted by an attorney who needed assistance, and that the employee should devote her full attention to the attorney's demands. The employee replied to the email, stating that she would assist in any way that she could.

Later the same day, the employee received a call from a man purporting to be the acquisition attorney. He asked the employee to process a wire transfer for him, on an urgent basis. A check, he said, would not suffice, due to the time constraints involved. The employee explained that under company protocol, she could not process such a transfer without several layers of authorization: she needed an email request from Medidata's president, as well as approval from the company's vice president and its director of revenue. In short order, the employee received just such an email, which was again by all appearances an authentic communication from Medidata's president. The email was copied to the company's vice president and director of revenue, and it informed the group that the president needed them to sign off on the transaction. In response, the accounts-payable employee initiated the transfer, which the vice president and director of revenue dutifully approved, resulting in a nearly $5 million wire transfer to the account that the "attorney" had provided.

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.

The wire-transfer request, of course, turned out to be fake. The company later learned that fraudsters had manipulated the Google Gmail platform that the company used for its emails by embedding a code into spoofed messages. The code essentially tricked the Gmail platform into recognizing the emails as intracompany communications, causing 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 funds transferred by Medidata could not be recovered from the perpetrators, as is typical in such situations, given that completed wire transfers usually cannot be reversed. The company therefore looked to its insurance policy as a potential source of recovery. In Medidata's case, that effort succeeded. The company was able to obtain coverage for its loss, as will be discussed below, but some others have not fared as well, because the policies to which insureds in such a situation will most likely turn have been found by a number of courts not to provide coverage for social engineering fraud. At a minimum, such claims are likely to involve disputed issues that make the availability of coverage far from a sure thing.

When faced with a wire-fraud loss, the first place to which a company will often turn is its crime policy. 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."

Potential Coverage Sources

When faced with a wire-fraud loss, the first place to which a company will often turn is its crime policy. 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."

"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, which take on different contours, depending on the precise policy language involved. One important overarching issue has emerged in a number of recent cases: whether a direct system intrusion or hacking is required for coverage, or whether a more human-oriented approach, in which thieves trick authorized users into effectuating transfers, will suffice.

"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.

"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.

Policies that provide coverage against cyber risks are another source to which policyholders may increasingly begin to turn, though obstacles are likely to be encountered there as well. Although cyber policies do not follow standardized forms—there is currently no ISO cyber coverage form, for example—such policies are often geared toward data breaches and other cybersecurity events rather than social engineering fraud, providing arguments that they are not designed to respond to this type of loss. Social engineering coverage that *is* expressly designed to respond to such losses may be available as an endorsement to a cyber or crime policy, but it is often subject to lower sublimits, creating an argument that if the policy responds at all, it is only within those limited confines. *See*, *e.g.*, *Travelers Cas. & Sur. Co. of America v. Hal Leonard LLC*, No. 2:2018cv00872, 2018 WL 2770946 (E.D. Wis.) (complaint filed June 8, 2018).

However, courts generally have not yet grappled with questions of coverage for social engineering losses under cyber policies or social engineering endorsements, making it difficult to predict how potential coverage arguments under those policies will be developed and resolved. This article will therefore focus on decisions that have addressed coverage for such losses under crime policies, with an eye toward providing insights into arguments that policyholders are likely to make, defenses that carriers may raise, and emerging trends in how courts have addressed these issues.

Computer Fraud Coverage

As noted above, the language of computer fraud coverage provisions can vary and may contain differing levels of specificity. These language variations have helped to shape courts' coverage inquiries, though important common threads and overarching issues have also emerged.

Was There "Use of a Computer" that "Directly" Caused the Loss?

A number of courts have addressed wire-fraud claims under policy provisions that covered loss of money "resulting directly from the use of a computer to fraudulently cause a transfer," or some similar variation. Some core issues that have arisen in these cases are whether fraudulent email correspondence constituted the sort of "use of a computer" contemplated by such language, and relatedly, whether such use was a sufficiently "direct" cause of the loss in question.

A key decision in this regard was the Fifth Circuit's ruling in *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016). The insured in that case, Apache, was an international oil-production company based in Houston. Apache received a call purportedly from one of its vendors, a company called Petrofac, and the caller instructed Apache to change the bank account information for its payments to Petrofac. Apache did not immediately comply, and instead informed the caller that the request had to be written on Petrofac's formal letter head. The following week, Apache received an email that appeared to be from Petrofac, though unbeknownst to Apache, the email was fraudulent and was from an email domain that looked similar to, but was not, Petrofac's real one. (Petrofac's true email domain was "petrofac.com," while the fraudulent email was from "petrofacltd.com.") The email had a signed letter attached, on what appeared to be Petrofac's letterhead, providing new bank account details.

An Apache employee attempted to verify the request by calling the phone number provided on the letterhead, which of course simply connected Apache to the fraudster. Apache did not take any other verification steps, but instead went on to implement the change and proceeded to pay real Petrofac invoices by transferring funds to the fraudster's account. Approximately $7 million was transferred before Apache discovered the fraud, and though some of the funds were recovered, Apache incurred a loss of about $2.4 million.

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[.]" *Apache*, 662 Fed. Appx. at 254. Though a Texas federal court found that there was coverage, the Fifth Circuit Court of Appeals reversed, holding that the fraudulent transfer was the result of other intervening events and was not caused "directly" by computer use. The only computer use was the email, to which was attached a letter on fraudulent letterhead, which had been sent at Apache's request in response to the initial telephone call. But this was just one step in the scheme, followed by numerous other events: Apache's "verification" by simply calling the telephone number provided (rather than independently confirming the request), Apache's act of changing the account information, and Apache's initiation of transfers to that account.

In the court's view, the email was merely incidental to the overall scheme. After all, electronic communications were ubiquitous by that time, and the court found that few, if any, fraudulent schemes would not involve *some* form of computer-facilitated communication. Rather, the end result came about because Apache ineffectively verified the request and authorized payment of a legitimate invoice to the wrong account. It was the invoices, the court found, and not the email, that were the reason for the transfers. *Apache*, 662 Fed. Appx. at 259*; accord Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co.*, 656 Fed. Appx. 332, 333 (9th Cir. 2016) (finding that computer fraud provision required some sort of hacking or unauthorized access, and explaining that "[b]ecause computers are used in almost every business transaction, reading [a computer fraud] 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," which the insured could not reasonably have expected).

However, another court examining similar policy language has recently come to a different conclusion. 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 for a scheme, much like the one in *Apache*, in which thieves created fraudulent emails that appeared to be from one of the insured's vendors. As in *Apache*, the 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 lower court, citing *Apache* and *Pestmaster*, adopted the view that the mere sending and receipt of fraudulent emails did not constitute "the use of any computer to fraudulently cause a transfer," and it found that something more akin to a system infiltration or "hacking" was required—using one computer to cause another computer to make an unauthorized, direct transfer of money. But the Sixth Circuit disagreed, finding that there was nothing in the policy's computer fraud language that expressly required hacking or unauthorized access. Noting that the insurer could have incorporated such language had it wished to do so, the court refused to find that the computer fraud provision was limited to hacking or similar behaviors.

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.

The court also found that the computer fraud was a sufficiently direct and immediate cause of the loss to trigger coverage. The loss itself was a "direct" one, the court found, since the insured lost its money as soon as the transfer to the thieves' account was effectuated; it was of no consequence that the insured also contractually owed (and later made partial payments of) those same sums to its vendor. And in the court's view, that "direct loss" was also "directly

caused" by the computer fraud. Though the court noted that there were "multiple internal actions" that the insured took after receiving the fraudulent emails—including determining which vendor invoices to pay, entering the fraudulent account information into a banking portal, and approving the payments—the court found that the computer fraud encompassed that whole chain of events. The court thus found that the insured suffered its loss "immediately after the transfer, which marked the end of the 'Computer Fraud' as defined in the policy." *American Tooling*, 2018 WL 3404708, at *5–6. *Cf. Interactive Communications Int'l, Inc. v. Great American Ins. Co.*, 2018 WL 2149769 (11th Cir. May 10, 2018) (finding that thieves' manipulation of a reloadable debit-card computer system to allow duplicate card redemptions constituted the fraudulent "use of a computer," but finding that the card issuer's loss did not "directly result" from this fraudulent use because a number of additional, intervening steps were required between the transfer of funds and the point when the insured actually lost all control over the funds).

Cases addressing this type of policy language have tended to focus on whether a fraudulent email constituted such an unauthorized "entry."

Was There an Unauthorized "Entry"?

Another "computer fraud" policy variant contains somewhat more specific language, requiring that a fraudulent transfer be effected not just by the use of a computer, but by an unauthorized "entry" or "introduction of instructions" into the insured's computer system. Cases addressing this type of policy language have tended to focus on whether a fraudulent email constituted such an unauthorized "entry." On a broad level, however, the core conceptual question raised by these cases is similar to that discussed above: whether some sort of direct hacking or unauthorized system intrusion is required for computer fraud coverage, or whether the sending of an email can suffice.

A key social engineering case addressing this policy language, *Taylor and Lieberman v. Federal Ins. Co.*, involved a scheme in which an accounting firm made wire transfers in response to emailed requests that appeared to be from a client, but in reality were generated by fraudsters who had taken control of the client's email account. 681 Fed. Appx. 627 (9th Cir. 2017). After the fraud was discovered, the insured sought coverage under a computer fraud provision that covered the taking of money resulting from an unauthorized "entry into" a computer system or "introduction of instructions" that propagated themselves through a computer system. The insured argued that the perpetrators' fraudulent emails satisfied this language: according to the insured, the emails themselves were an unauthorized "introduction of instructions" or "entry into" its computer system. The Ninth Circuit rejected this argument, however, finding that simply sending an email did not constitute an "unauthorized entry" into a computer system, at least in the absence of some interference with the computer's functioning. Similarly, the court found that the emails were not an unauthorized "introduction of instructions" that propagated themselves through the system. The emails had instructed the insured to initiate wire transfers, but the court found that under a common sense reading of the policy, these were not the types of "instructions" that the policy was designed to cover. Rather, interpreting the policy language in its ordinary sense, it required something more akin to the introduction of malicious computer code that "propagated" itself through the system, such as a virus. Instructions that were directed to the insured as part of the text of an email, the court found, did not suffice.

Similarly, in *Universal American Corp. v. National Union Fire Ins. Co.*, 25 N.Y. 3d 675 (NY App. 2015), the Court of Appeals of New York found that health-care providers' submission of fraudulent Medicare claims to a health insurer's computerized billing system was not "fraudulent entry of electronic data," as was required for the insured's computer fraud coverage to apply. The court interpreted the policy to require that the *entry into the system itself* be fraudulent—in other words, a hacking of the computer system—rather than an authorized entry of *information* that was fraudulent. In the court's view, the wording of the policy, including the "intentional word placement of 'fraudulent' before 'entry' and 'change,'" manifested the parties' "intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access." *Id.* at 681. Because the health-care providers who submitted fraudulent claims were authorized to use the computer billing system, the computer fraud coverage did not apply.

The court in the *Medidata* case, on the other hand, reached a somewhat different result. The policy in that case covered the "direct loss" of money resulting from "computer fraud," which was defined to include a transfer resulting from "the fraudulent (a) entry of Data into… a Computer System;" or "(b) change to Data elements or program logic of a Computer System[.]" *Medidata*, 2017 WL 3268529. As discussed above, the perpetrators used computer code to trick Medidata's Gmail platform into populating spoofed emails with the company president's name and email address, and Medidata argued that this constituted fraudulent "entry" and "change" of data in its computer system. The court agreed with Medidata, finding that the thieves' actions involved the kind of "deceitful and dishonest" access that the Court of Appeals of New York had envisioned in *Universal American Corp.* Hacking, the court found, was just one of many methods that a thief could use, and it was simply an everyday term for "unauthorized access to a computer system." The perpetrators' messages were embedded with computer code that interacted with the Gmail system to change the information that was displayed, and the court found that this "violat[ion] of the integrity of the computer system through unauthorized access" was enough to constitute "computer fraud." Moreover, the court held that there was a sufficiently direct causal nexus between the email spoofing and the transfers, finding that

"Medidata employees only initiated the transfer as a direct cause of the thief sending spoof e-mails posing as Medidata's president."

The Second Circuit Court of Appeals recently affirmed the *Medidata* decision, agreeing with the district court that the plain and unambiguous language of the policy covered Medidata's loss. *See* 2018 WL 3339245 (2d Cir. July 6, 2018) (summary order). Though no hacking had occurred per se, the court found it significant that the fraudsters had nevertheless crafted a "computer-based attack" that manipulated Medidata's email system (which was undisputedly a "computer system" within the meaning of the policy). The introduction of spoofing code into the system, the court found, represented a "fraudulent entry of data," and moreover was a "change to [a] data element" as the code altered the email system's appearance. The court also agreed that the spoofing attack was a sufficiently proximate cause of Medidata's loss, finding that although Medidata employees had to take action to effectuate the transfer, their actions were not sufficient to sever the causal chain.

Notably, the court also distinguished Medidata's loss from a situation (such as the one in *Universal American Corp.*) in which computers were implicated merely because that was the medium through which the fraudulent information happened to be sent. Unlike a *Universal*-type scenario, the court found, the Medidata fraud implicated the "computer system qua computer system," since it was Medidata's email system itself that was compromised.

Computer Fraud Takeaways

As the above cases demonstrate, the contours of courts' analyses vary depending on the policy language in question, and they can be quite fact specific as well. On a broad level, however, an overarching conceptual issue appears to drive many of the holdings in these cases: can computer fraud coverage be triggered by a fraud scheme that involves the use of computers on some level, but which is ultimately aimed at tricking a human victim, whose intervention is needed to accomplish the transfer of funds? Or is such coverage limited to situations in which it is the computer itself that is the target, such as when a thief hacks into a computer system to initiate a transfer of funds directly?

Results are not uniform, and the state of the law is clearly in some degree of flux. At least until recently, there appeared to be some trend toward the latter approach—providing coverage for hacking or other system interference that directly triggers a transfer or "defrauds" a computer system itself, but not extending coverage for human error in succumbing to a fraud scheme, as reflected in the *Apache*, *Taylor and Lieberman*, and *Universal American* decisions. In addition to the rationales discussed in those cases, such an approach is arguably most consistent with certain underwriting and public policy considerations that may be implicated by these issues. One commentator has suggested, for example, that computer fraud provisions are underwritten to cover hacking-induced transfers that are arguably further outside of an insured's control than are internal, employee-related risks, and that while broader fraud coverage could be written, it would involve a different level of risk and higher premiums than the insured has paid. *See* Br. for the Surety & Fidelity Ass'n of Am. as Amicus Curiae, filed on Mar. 20, 2015, in *Pestmaster*, No. 14-56294, 656 Fed. Appx. 332 (9th Cir. 2016). The availability of social engineering fraud endorsements that are subject to lower sublimits (and additional premium) appears to be consistent with such an argument, though it remains to be seen how courts will address coverage disputes under policies containing such endorsements.

The recent *American Tooling* and *Medidata* decisions, however, have made the picture more textured. For policies that contain a more general definition of computer fraud, the Sixth Circuit's holding in *American Tooling* appears to represent a different approach than the one taken by the Fifth Circuit in the *Apache* case. It will be important to see how other courts respond, and whether they are more inclined to apply the logic of the *Apache* decision—declining to interpret the provision in a manner that might broaden it into coverage for "general" fraud—or whether they are willing to find the provision ambiguous and construe it in favor of coverage.

The *Medidata* case appears to reflect a somewhat different approach from other decisions that have interpreted the more detailed computer fraud language found in that policy. Given the court's focus on the email-tampering element of the scheme, however, it is not clear whether *Medidata* represents a departure from the view that some form of "hacking" is required for computer fraud coverage, or whether it will be viewed as something of a middle ground—perhaps paving the way for a distinction between social engineering schemes that are accomplished via actual compromises of the insured's computer system, as opposed to those in which email is simply used as the vehicle for sending an otherwise fraudulent message. Regardless, as with *American Tooling*, it will be important to observe how other courts interpret the *Medidata* holding, and whether it comes to represent a shift or merely a nuance in the developing wire-fraud coverage landscape.

Regardless, as with *American Tooling*, it will be important to observe how other courts interpret the *Medidata* holding, and whether it comes to represent a shift or merely a nuance in the developing wire-fraud coverage landscape.

Funds Transfer Fraud Coverage

Another provision typically included in a crime policy to which an insured may turn after suffering a social engineering loss is a provision for "funds transfer fraud" coverage. As with computer fraud provisions, there are some variations in the text of the

provisions themselves, but several common issues have developed in the case law.

Is a Fraudulently Induced Wiring Instruction an Instruction Made with the Insured's "Knowledge and Consent?"

Traditionally, funds transfer fraud coverage has been interpreted to apply to losses resulting from fraudulent transfer instructions sent by a third party to a financial institution without the knowledge or consent of the insured, directing the institution to disburse funds from the insured's account. Decisions outside of the social engineering context have often concluded that coverage did not extend to claims involving a transfer authorized by the insured, even if the transfer was associated with some sort of fraudulent scheme.

A good example of the "authorized transaction" analysis is found in *Pestmaster Servs. Inc. v. Travelers Cas. and Sur. Co. of America*, in which 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 insured had executed an authorization that permitted the administrator to initiate an Automated Clearing House (ACH) transfer from the company's bank account to pay approved invoices. The administrator would issue weekly invoices reflecting amounts for payroll and payroll taxes, and after approval by the company, the administrator would initiate ACH transfers from the company's account to cover the amounts due. A surprise visit by the I.R.S. revealed that the administrator had failed to make payroll tax payments and that the insured now owed almost $400,000 in back taxes.

The insured sought coverage under a funds transfer fraud provision in its crime policy that covered "direct loss of Money and Securities contained in [the company's] Transfer Account on deposit at a Financial Institution directly caused by Funds Transfer Fraud." The policy defined "Funds Transfer Fraud" to include:

> a fraudulent written instruction… issued to a Financial Institution directing such Financial Institution to… transfer… Money… by use of an electronic transfer system at specified intervals or under specified conditions which written instruction purports to have been issued by you but was in fact fraudulently issued, Forged or altered by someone other than you without your knowledge or consent.

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)). Because the funds at issue had been transferred with the insured's express authorization, and there was no evidence that the payroll administrator or any third party "gained unauthorized entry into [the insured's] bank's electronic fund transfer system or pretended to be an authorized representative or otherwise altered the electronic instructions in order to wrongfully divert money from the rightful recipient," the *Pestmaster* court concluded that there was no coverage for the insured's loss.

The Ninth Circuit generally followed this approach in determining that no coverage was available under a funds transfer fraud provision for losses incurred by an accounting firm that had wired funds in reliance upon emails that appeared to have been sent by its client but that turned out to be fraudulent. *See Taylor & Lieberman v. Federal Ins. Co.*, *supra* (addressing funds transfer fraud coverage provision, in addition to the "computer fraud" provision discussed above). The funds transfer fraud provision extended coverage to "fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution transfer… Money… from any account maintained by an Insured Organization at such Institution, without the Insured Organization's knowledge or consent." The court held that the provision was inapplicable to the loss because the accounting firm "requested and knew about" the wire transfer, notwithstanding that the emailed instructions had been fraudulent. The court also rejected the firm's argument that the emails themselves triggered coverage, reasoning that the insured accounting firm that received and relied upon them was not a "financial institution" as required under the policy language.

The court in *Medidata* also addressed a funds transfer fraud provision and applied the "authorized transaction" analysis to facts very similar to *Taylor & Lieberman*, yet came to a very different result, finding that coverage existed for losses associated with a social engineering scheme, despite the fact that the wiring instruction at issue technically had been authorized by the insured. *See* 268 F. Supp.3d at 480. The funds transfer fraud provision at issue provided coverage for "fraudulent electronic… instructions… purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer… Money… from any account maintained by such Organization at such institution, without such Organization's knowledge or consent." The insurer argued, based upon *Pestmaster*, that no coverage was available because the transfer instructions were valid and had been sent with the knowledge and consent of the accounts payable employee.

The *Medidata* court rejected this argument, distinguishing the situation before it from the facts of *Pestmaster*, which it characterized as involving "valid electronic transfers to [the] payroll administrator who later misappropriated the funds." *Id.* Unlike the situation in *Pestmaster*, the court observed, a third party had impersonated an authorized representative and directed the accounts payable employee to initiate the wire transfer, which would not have been made absent the manipulated emails. In the court's view, the fact that the employee willingly pressed the send button did not transform the transfer into a valid transaction. Rather, "the validity of the wire depended upon several high level employees' knowledge and consent, which was only obtained by trick. As the parties are well aware, larceny by trick is still larceny." *Id.* The *Medidata* court thus concluded that the insured had established its

entitlement to coverage under the funds transfer fraud provision.

Although the *Medidata* decision was affirmed on appeal, the Second Circuit did not pass on the district court's analysis of coverage under the funds transfer fraud provision, instead relying on the computer fraud provision of the policy to sustain the judgment in favor of the insured, as discussed above. *See Medidata*, 2018 WL 3339245. Thus, there remains a lack of uniformity in the case law concerning the "authorized transaction" issue in the context of social engineering, which is still in its infancy. It remains to be seen whether the *Taylor & Lieberman* approach, the *Medidata* approach, or even some other approach will prevail.

Did the Loss Result "Directly" from a "Fraudulent Instruction?"

Another issue that can arise when coverage is sought for social engineering fraud is how directly connected the loss must be to the fraudulent transfer instruction. While many policies limit coverage to losses "resulting directly" from a fraudulent instruction, the term "fraudulent instruction" is sometimes defined broadly enough to include emails sent by a fraudster. Disputes can arise about whether social engineering schemes, which often involve a multi-step process with several rounds of interactions, fit within this language.

Such was the case in *Principle Solutions Group, LLC v. Ironshore Indem. Inc.*, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016), in which the court considered whether a company that had been victimized by social engineering fraud was entitled to coverage under a "computer and funds transfer fraud" provision of its crime policy. The fraud in *Principle* followed a common pattern: an employee, this time the company's controller, received a spoofed email, ostensibly from the company's president, advising her that her assistance was needed to close on acquisition and instructing her to work with the company's outside counsel and to ensure a wire transfer was processed that day. Shortly thereafter, the controller was contacted by an imposter posing as the company's attorney, who verbally requested a wire transfer on an urgent basis and provided wiring instructions. The controller oversaw and approved the issuance of the wire-transfer instructions, affirming that they were valid when the bank requested confirmation, only to learn the following day that the company had been defrauded.

The computer and funds transfer fraud provision provided coverage for "Loss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer… 'money'… from that account." The term "fraudulent instruction" was defined by the policy to include an "instruction initially received by you, which instruction purports to have been issued by an 'employee', but which was fraudulently issued by someone else without your or the employee's knowledge or consent." The company asserted that the loss resulted directly from the fraudulent email purportedly sent by the company's president. The insurer argued that the loss was not directly tied to the initial email because the information for the wire transfer had been provided by the imposter posing as outside counsel, and the company's employees had set up and approved the transfer.

The *Principle Solutions* court found that the language of the computer and funds transfer fraud provision was ambiguous, in that a reasonable insured could interpret it as providing coverage even if there were intervening events between the fraud and the loss. Citing the *Apache Corp.* decision discussed above, the court rejected the insurer's position that an immediate link between the injury and its cause was required, as this would "limit the scope of the policy to the point of almost nonexistence." *Id.* at *5. Because the company could only act through its employees, the court reasoned, some employee interaction between the fraud and the loss must be allowed, otherwise the provision would be rendered "almost pointless" and any coverage would be rendered illusory. While not specifying what amount or type of employee interaction would be acceptable, the court ruled that the company was entitled to coverage under the computer and funds transfer fraud provision.

The *Principle Solutions* decision is currently on appeal to the Eleventh Circuit Court of Appeals and has been scheduled for argument in November 2018. While several other decisions have addressed the "directness" issue in the context of a computer fraud provision, *Principle Solutions* appears to be the only decision to address "directness" in the context of a funds transfer fraud provision, and the Eleventh Circuit's decision is likely to play a significant role in shaping this area of the law.

While many policies limit coverage to losses "resulting directly" from a fraudulent instruction, the term "fraudulent instruction" is sometimes defined broadly enough to include emails sent by a fraudster.

Funds Transfer Fraud Takeaways

The case law concerning coverage for social engineering losses under funds transfer fraud provisions is far from settled. In view of the willingness of some courts to relax policy requirements and to find in favor of the insured, it appears likely that this will be a fertile area for litigation in the future. As shown in the *Taylor & Lieberman* and *Medidata* cases, the "authorized transaction" analysis may not be the most useful approach for analyzing coverage for social engineering losses. It remains to be seen whether courts will continue to use this analysis—and if so, what level of knowledge will be required for the insured's authorization to be considered valid and thereby preclude coverage—or whether courts will instead develop a different test. Future decisions in this area will similarly need to address the issue of "directness," which can be problematic in social engineering fraud cases, because a loss may be three or four steps removed from the event that otherwise brings the claim within the policy language. Here again, the existence of coverage may turn upon a court's will-

ingness to relax more traditional analytical concepts or to modify them to account for the somewhat unique circumstances posed by social engineering fraud.

Forgery and Alteration Coverage

Unlike victims seeking coverage for social engineering losses under "computer fraud" and "funds transfer fraud" provisions, insureds seeking coverage for such losses under "forgery and alteration" provisions have seen their claims uniformly rejected by the courts. The reason for this is that such provisions invariably require that there be a forgery or alteration of some sort of financial instrument, which normally does not happen in a social engineering scheme. 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.

For example, in *Medidata*, although the court found coverage for social engineering losses under both computer fraud and funds transfer fraud provisions, it nevertheless refused to find that the policy's forgery coverage was triggered. *See* 268 F. Supp. 3d at 480. The forgery provision required "direct loss resulting from Forgery or alteration of a Financial Instrument committed by a Third Party." After noting that the parties' disagreed on whether the spoofed emails that induced the insured to wire funds to the fraudster constituted a forgery, the court held that a forgery, even if proved, would be immaterial, because it was undisputed that there was no financial instrument involved in the scheme, which was fatal to the coverage claim. The court rejected as "strained" the insured's suggestion that forgery alone, without a financial instrument, was sufficient to trigger coverage, because that would convert the provision into a general crime policy.

Interpreting an identical provision, the court in *Taylor & Lieberman* also ruled against an insured accounting firm seeking coverage for social engineering losses due to the absence of a financial instrument. *See* 681 Fed. Appx. at 628. The court observed that the fraudulent emails instructing the accounting firm to wire client funds did not constitute financial instruments "like checks, drafts, or the like" within the meaning of the policy. Even if they were considered the equivalent of checks or drafts, they were not "made, drawn by, or drawn upon" by the insured firm as required under the relevant definition. Instead the emails directed the firm to wire money from its client's account. As such, there could be no coverage under the forgery provision.

Forgery and Alteration Takeaways

Insureds seeking coverage under forgery and alteration provisions face an uphill battle. By their nature, social engineering scams are unlikely to involve a financial instrument, and courts have not been receptive to arguments that fraudulent emails received by an insured are equivalent to the forgery of a financial instrument that is needed to trigger coverage. Given the difficulty of satisfying these requirements, an insured is likely better served focusing resources on securing coverage under different provisions, if possible.

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. FD