COVINGTON

Federal Courts of Appeals Clarify Scope of Computer Fraud Coverage

July 24, 2018

Insurance Recovery

Phishing, spoofing, and computer-based scams pose a significant threat to businesses. Yet in recent years many victims of these scams — also variously referred to as "business email compromise," "social engineering," "fake creditor," or "fake president" fraud — have found that their insurers refused to pay claims for their computer-related fraud losses. Policyholders will thus welcome two recent federal courts of appeals decisions — *Medidata Solutions Inc. v. Federal Insurance Co.*, No. 17-2492, 2018 WL 3339245 (2d Cir. July 6, 2018), and *American Tooling Center, Inc. v. Travelers Casualty & Surety Co. of America*, No. 17-2014, 2018 WL 3404708 (6th Cir. July 13, 2018) — upholding coverage for these types of computer fraud. In these two cases, the courts rejected insurers' attempts to limit coverage for computer fraud based on the "direct loss" requirement in their policies. In doing so, they held that computer fraud coverage under common commercial crime policies is not limited to direct "hacking," but also applies when email spoofing causes the policyholder's employee to transfer funds to a fraudster impersonating an executive or vendor.

These recent decisions are encouraging news for policyholders already embroiled in insurance coverage disputes over social engineering fraud losses. The safer course for policyholders, however, is to scrutinize any policy language relating to computer, business email compromise or social engineering fraud before a loss arises. Both the language of the policies and the techniques of the fraudsters are constantly evolving. For this modern-day fraud risk, the advice of experienced coverage counsel and a sophisticated broker before the insurer issues a policy may save much time and expense after the policyholder suffers a fraud loss.

The Second Circuit's *Medidata* Decision

In *Medidata*, employees of the policyholder company transferred more than $5 million as a result of fraudulent email instructions that appeared to come from high-ranking members of the organization. Medidata sought coverage under its executive protection portfolio policy, which included computer fraud coverage. The insurer denied the claim, arguing that there was no covered loss. The Second Circuit disagreed.

First, the Second Circuit rejected the insurer's argument that the spoofing attack did not fall within the grant of coverage for losses stemming from any "'entry of Data into' or 'change to Data elements or program logic of' a computer system." The court explained that "[w]hile Medidata concedes that no hacking occurred, the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system." According to the court, "the attack represented a fraudulent entry of data into the computer system, as the spoofing code was

introduced into the email system," and "[t]he attack . . . made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender."

Second, the Second Circuit held that employees transferring funds pursuant to the fraudulent email instructions resulted in a "direct loss." Applying New York law interpreting "direct loss" to mean "a proximate cause," the court concluded that the spoofing attack proximately caused the loss. Although authorized Medidata employees themselves transferred the funds, that did not interrupt the chain of causation between the initial fraud and the ultimate loss. In the words of the Court, "[t]he chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred. The employees were acting, they believed, at the behest of a high-ranking member of Medidata. And New York law does not have so strict a rule about intervening actors as [insurer] argues."

The Sixth Circuit's *American Tooling Center* Decision

In *American Tooling Center*, a third party impersonating American Tooling Center's ("ATC's") vendor intercepted emails requesting the vendor's invoices for payment. By email, the impersonator instructed ATC's employee to wire payments to various accounts over the next few months. The employee, believing the instructions to be genuine, transferred approximately $834,000 to the new bank accounts before others at the company determined that the emails requesting payment to the new accounts were fraudulent. ATC then paid the actual vendor 50% of the invoice amounts that the wires were intended to pay, and the vendor agreed that the remaining 50% would be contingent on ATC's insurance recovery. ATC sought payment from Travelers under its computer crime/fraud coverage. Travelers denied the claim.

On the "direct loss" issue, the Sixth Circuit held that, under Michigan law, "direct" meant an immediate or proximate cause, rather than a remote or incidental cause. Applying this standard, the court held that the policyholder immediately lost its money when it paid $834,000 to the impersonator. The court rejected the insurer's argument that the loss resulted from the policyholder's agreement to pay the vendor at least half of the money still owed. The court explained: "A simplified analogy demonstrates the weakness of Travelers' logic. Imagine Alex owes Blair five dollars. Alex reaches into her purse and pulls out a five-dollar bill. As she is about to hand Blair the money, Casey runs by and snatches the bill from Alex's fingers. Travelers' theory would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill. This interpretation defies common sense."

The Sixth Circuit likewise held that the policyholder suffered its loss immediately after transferring funds. The court distinguished the Eleventh Circuit's recent decision in *Interactive Communications International, Inc. v. Great American Insurance Co.*, No. 17-11712 (May 10, 2018). There, the loss resulted from holders of prepaid debit cards who exploited a coding error in the insured's computer system to fraudulently increase the balances on their cards. The Eleventh Circuit panel held that this loss was not directly caused by computer fraud. That case, the Sixth Circuit noted, provided a "helpful counterpoint" because the loss resulted from a multi-step, multi-actor process. Indeed, in *Interactive Communications*, the Eleventh Circuit acknowledged that the loss would have been "directly caused by" fraud if the "point of no return"

— when the policyholder could no longer recover its money — occurred immediately after the fraud, instead of at a later time when the bad actors made purchases using the debit cards and third parties deducted funds from the policyholder's account.

The Sixth Circuit in *American Tooling Center* further rejected the insurer's argument that the policy's definition of "Computer Fraud" requires the fraudster himself to effect the actual computer funds transfer. The court made clear that the policy's "Computer Fraud" coverage was not limited to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer."

Other Pending Computer Fraud Coverage Cases

Similar cyber fraud coverage disputes are pending in other cases before federal courts. For example, in *Principle Solutions Group LLC v. Ironshore Indemnity Inc.*, No. 15-cv-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016), the district court found coverage under a commercial crime policy, and the insurer's appeal is now before the Eleventh Circuit (No. 17-11703). In that case, the policyholder Principle Solutions Group LLC ("Principle") wired $1.7 million to a sham bank account after one of its employees received an email purportedly from a Principle executive about working with a lawyer to transfer funds for an acquisition. The purported executive and attorney, however, were fraudsters. Principle's policy covered "computer and funds transfer fraud" losses "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. Principle's insurer contended that Principle's loss did not result directly from the fraudulent instruction in the initial email, because there were intervening acts between that email and the wire transfer. In granting Principle summary judgment, the district court concluded that the policy term "loss resulting directly" was ambiguous and therefore must be interpreted in Principle's favor. The district court also recognized that "[i]f some employee interaction between the fraud and the loss was sufficient to allow [an insurer] to be relieved from paying under the provision at issue, the provision would be rendered 'almost pointless' and would result in illusory coverage." The Eleventh Circuit has not yet heard argument, but the policyholder has recently submitted the *Medidata* and *American Tooling Center* decisions as supplemental authorities for its position.

Takeaways

Medidata and *American Tooling Center* give policyholders a valuable argument: when policyholders' employees are duped into making payments through phishing, spoofing, or other computer-related frauds, the "direct loss" requirement should not bar computer fraud coverage.

They also highlight the prevalence of coverage disputes under common commercial crime policies regarding fraud losses from email spoofing scams. Since these coverage issues first emerged, many insurers have endorsed or amended their policies to exclude business email compromise risk specifically — or alternatively to cover it specifically, for an additional premium or with a small sublimit. These newly minted "social engineering" endorsements are neither uniform nor always skillfully drafted; meanwhile the spoofing/social engineering fraud techniques continue to evolve. Therefore, the coverage disputes going forward may turn on the interpretation of highly specialized policy terms and their application to highly specific fact patterns.

To reduce the likelihood of such coverage disputes, prudent policyholders should pay careful attention both to their vulnerability to this 21st-century fraud risk and to appropriate risk management measures. With the assistance of experienced coverage counsel and brokers, policyholders should scrutinize both their crime and their cyber insurance programs at renewal time, to determine whether they afford adequate protection for email spoofing or similar social engineering fraud losses. If not, they should be prepared to negotiate amendments or clarifications of inartful standard wordings; to insist on adequate sublimits; to survey the market for purpose-built specialty coverage; or, if necessary, to take appropriate steps to self-insure the risk of computer fraud.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Insurance Recovery practice:

John Buchanan	+1 202 662 5366	jbuchanan@cov.com
Gretchen Hoff Varner	+1 415 591 7056	ghoffvarner@cov.com
René Siemens	+1 424 332 4751	rsiemens@cov.com
Matt Schlesinger	+1 202 662 5581	mschlesinger@cov.com
Mark Herman	+1 202 662 5758	mherman@cov.com
Tara Brennan	+1 202 662 5588	tbrennan@cov.com