COVINGTON

Recent Cases on E-Mail "Spoofing" Coverage Highlight the Impact of Specific Crime Policy Wordings

August 16, 2017

Insurance Recovery

Two recent federal district court decisions involving computer "spoofing" scams highlight the uncertainty about whether such incidents may be covered under standard "computer fraud" provisions in widely used crime insurance forms. The conflicting results in these cases provide a stark reminder to policyholders that seemingly minor differences in policy wordings can have a major impact on the scope of coverage – and severe financial consequences.

"Spoofing" refers to the practice of manipulating a commercial e-mail to falsify the e-mail's true origin, without the consent or authorization of the user whose e-mail address is "spoofed." *See Karvaly v. eBay, Inc.*, 245 F.R.D. 71, 91 n.34 (E.D.N.Y. 2007). As recent cases reflect, scam artists have used spoofing—also known as "business email compromise," "social engineering," or "fake president" fraud—to induce even high-level executives of sophisticated companies to transfer millions of dollars to accounts under the scammers' control. Faced with irretrievable losses, many companies have understandably looked first to the "computer fraud" and other provisions of their corporate crime policies for insurance coverage.

Last month, in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 2017 WL 3268529, __ F. Supp. 3d __ (S.D.N.Y. July 21, 2017), the court found coverage under the "computer fraud" provision of the insured's crime policy for a $4.8 million loss resulting from an email spoofing scam. The scam started with a spoofed email to an accounts payable employee purportedly from Medidata's president, directing the employee to await an attorney's wire transfer instructions to pay for an impending acquisition. *Id.* at *1. That same day, the purported attorney called with instructions to process the wire transfer, and a subsequent spoofed email induced both Medidata's vice-president and its CFO to sign off on the transfer. *Id.* at *2. Not until two days later did the company realize that it had been defrauded. *Id.*

Less than two weeks after the *Medidata* decision, however, the district court in *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*, No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017), considered a computer-fraud claim based on a strikingly similar spoofing scam, and reached the opposite conclusion. In *ATC*, the spoofed email came in apparent response to the insured's request to a vendor for invoices confirming the completion of certain production milestones under the vendor's contract. The email instructed ATC to wire payment to a new bank account. An ATC executive verified that the milestones had in fact been met, but did not validate the new bank instructions before authorizing an $800,000 wire transfer to what ATC later learned was a fraudulent account. *Id.* at *1.

The crime policy at issue in *ATC* covered "direct loss" of money or other property "directly caused by Computer Fraud," defined as the "use of any computer to fraudulently cause a

transfer" of money or other property from within the insured entity to a third party. The court reasoned that the loss to ATC was not "directly caused" by "Computer Fraud," because the executive's verification of production milestones and authorization and initiation of the transfers constituted "intervening events" between the "use" of a computer and the actual loss. *Id.* at *2. Thus, "[t]he emails themselves did not directly cause the transfer of funds," but only contained the information on which the insured relied to intentionally, albeit unwittingly, authorize the transfer. *Id.* at *3.

ATC is the latest in a string of cases denying computer-fraud coverage on the grounds that spoofed emails did not involve an infiltration or "hacking" of the insured's computer system and were therefore merely incidental to the loss. *See*, *e.g., Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016); *Pestmaster Servs., Inc. v. Travelers Cas. & Surety Co.*, 656 Fed. Appx. 332 (9th Cir. 2016). One of these recent rulings is currently on appeal in the 11th Circuit: *Incomm Holdings, Inc. v. Great Am. Ins. Co.*, 2017 WL 1021749 (N.D. Ga., March 16, 2017), *appeal pending,* No.17-11712 (11th Cir.).

Medidata, however, should not be regarded as a mere outlier. Rather, the pro-coverage result in *Medidata* highlights the power of subtle differences in policy wordings to materially alter the scope of available coverage.

Though Medidata's crime policy covered only "direct loss," it defined "Computer Fraud" more broadly as "the unlawful taking *or the fraudulently induced transfer*" of money or other property "resulting from a Computer Violation," including both fraudulent "entry of Data into . . . a Computer System" and "change to Data elements or program logic of a Computer System" directed against the insured. 2017 WL 3268529, at *2. Unlike the *ATC* policy, the *Medidata* policy did not specify that the computer violation itself must "directly" cause the loss. Medidata demonstrated that the thief had masked the fraudulent emails' true origin using an embedded computer code, which the insured's email system processed upon receipt to insert the name and photo of its president. Under these circumstances, the *Medidata* court had no trouble concluding that a transfer fraudulently induced by such manipulated emails resulted in a "direct loss" under this policy.

In reaching this conclusion, the *Medidata* court also distinguished or disagreed with the reasoning of *Apache*, *Pestmaster*, and other decisions denying computer-fraud coverage for a variety of computer-related schemes. The court appears to have been persuaded that sending a manipulated e-mail armed with deceptive code to the insured is not an "authorized" access to the insured's computer system, and a transfer of money resulting from such deceit is not genuinely "authorized" by the insured. A loss thus remains "direct" in nature if the deception continues throughout any intervening steps between receipt of the spoofed email and the transfer of funds.

Medidata underscores not only the importance of favorable coverage-grant wording but also the need to support a computer-fraud claim with technical evidence tailored to the precise requirements of that wording. E-mail scams are constantly evolving. In *Medidata*, the specific operation of the embedded code in the spoofed email was key to demonstrating that the fraud involved more than just a deceptive textual message, but actually misappropriated and altered data within the insured's e-mail system. Only by detailing these technical steps was the insured able to establish that the trickery met the policy definition of a computer violation.

In light of recent developments in this area, policyholders should review their crime policies for key wordings that may exclude spoofing and other fraudulent inducement schemes, and seek appropriate coverage enhancements in the next renewal cycle. If sufficiently broad wording cannot be obtained, explicit "fraudulent impersonation" or "social engineering" coverage should also be considered as an add-on to the insured's regular crime, fidelity, or cyber policies—but these coverage extensions also must be carefully vetted to ensure sufficient breadth and dollar limits to justify their additional premium cost.

Given insurers' track record to date in resisting coverage for business email scams, one thing is certain: policyholders should not simply assume that an off-the-shelf crime insurance policy form will protect them if their employees fall prey to spoofing or other fraudulent email scams.

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

Mitchell Dolin	+1 202 662 5210	mdolin@cov.com
Benedict Lenhart	+1 202 662 5114	blenhart@cov.com
P. Benjamin Duke	+1 212 841 1072	pbduke@cov.com
Matt Schlesinger	+1 202 662 5581	mschlesinger@cov.com
René Siemens	+1 424 332 4751	rsiemens@cov.com
Richard Mattick	+44 20 7067 2023	rmattick@cov.com
Scott Levitt	+1 202 662 5661	slevitt@cov.com