New York Law Journal

SERVING THE BENCH AND BAR SINCE 1888

WWW.NYLJ.COM An ALM Publication

VOLUME 258—NO. 56 WEDNESDAY, SEPTEMBER 20, 2017

SDNY Finds Coverage for Payment Instruction Fraud Loss

By **Howard B. Epstein**

And **Theodore A. Keyes**

A fraudster impersonating either a company executive or an outside vendor communicates a request for funds, usually by email, to an employee with the authority or ability to perform the transaction. Too often, the employee falls for the scheme, fails to verify the request and the money is long gone by the time the company discovers that it has been defrauded. Call it what you will—payment instruction fraud, social engineering fraud, imposter fraud, vendor fraud, fake president fraud, business email compromise scam—there are many labels for the conduct and an even larger variety of schemes through which criminals have sought to defraud companies by persuading employees to unwittingly transfer company funds to accounts controlled by the criminals.

Where the lost funds are significant, companies have sought to recover the loss from their insurers under the computer fraud coverage section of their crime insurance policies. These insurance claims have sprouted a series of lawsuits across the country between the insurance companies and their insureds. Typically, the insurers have denied the claims if the use of the computer in the scheme was limited simply to communication by email. The insurers have taken the position that computer fraud coverage does not respond unless there is some computer activity integral to the scheme—such as hacking or other infiltration of the computer system—above and beyond mere email communications from the fraudster to the company employees. Court decisions have been less than a model of consistency, in part because the governing policy language can vary from policy to policy.

> Court decisions have been less than a model of consistency, in part because the governing policy language can vary from policy to policy.

In late July, the Southern District addressed an insurance dispute over loss incurred due to a payment instruction fraud. In *Medidata Solutions v. Federal Insurance*, 2017 WL 3268529 (S.D.N.Y. July 21, 2017), the Southern District ruled in favor of the insured, finding coverage under both the Computer Fraud and the Funds Transfer Fraud sections within the Crime Coverage of the Executive Protection insurance policy. In so ruling, the district court relied on the specific details of the scheme as well as the specific language of the insurance policy.

Medidata Is Defrauded

Medidata Solutions provides cloud-based services for the use and storage of data related to clinical trials. In the summer of 2014, Medidata notified its finance department that its short-term business plan included a possible acquisition and that personnel should be prepared to assist with "significant transactions on an urgent basis." Id.

In September 2014, a finance department employee responsible for processing travel and entertainment expenses received an email, purportedly from the president of Medidata, explaining that Medidata was close to finalizing a confidential acquisition and that she should devote her full attention to the instructions that she would be receiving from an attorney involved in the transaction. The "From" field in the email message contained the president's name, email address and picture.

On the same day, the finance department employee received a telephone call from the purported attorney who demanded that she process a wire transfer. She explained that, before processing a wire transfer, she needed an email

HOWARD B. EPSTEIN *is a partner at Schulte Roth & Zabel, and* THEODORE A. KEYES *is special counsel at the firm.*

request from Medidata's president and approvals from the vice president and the director of revenue. Subsequently, the vice president, director of revenue and the finance department employee received a group email, purportedly from the president, instructing that the requested wire transfer be approved and processed. The group email message again contained the president's email address in the "From" field and his picture next to his name. In response, the finance department employee logged on to the on-line banking system, submitted the wire transfer for approval and the vice president and director of revenue approved the transfer, wiring $4,770,226 to an account based on the instructions received from the purported attorney.

A couple of days later, the purported attorney again contacted the finance department employee and requested a second wire transfer. The employee began processing the transfer and the director of revenue approved it. This time, however, the vice president held up the transfer because he thought the email address in the "Reply To" field looked suspicious. Following discussion, the employee sent a separate email to the president inquiring about the wire transfers and learned that the president had not requested either transfer. At that point, company officials realized that they had been defrauded. Medidata contacted the FBI and hired outside counsel to conduct an investigation, which revealed that an unknown actor had altered the emails to appear as if they were sent from Medidata's president.

Summary Judgment Granted

Medidata sought coverage for its losses under the Crime Coverage section of the insurance policy issued by Federal Insurance Company. Specifically, Medidata sought coverage under the Computer Fraud, Funds Transfer Fraud and Forgery coverage sections of the policy. Federal denied the claim under each of the coverage sections, leading Medidata to file a lawsuit. Id.

Initially, both Medidata and Federal filed motions for summary judgment. The district court denied both motions without prejudice on the grounds that the record was insufficient and granted the parties leave to conduct limited expert discovery. According to the court's order, expert discovery was to be limited to "establishing the method in which the perpetrator sent its emails to plaintiff and discussing what changes, if any, were made to plaintiff's computer systems when the emails were received." *Medidata Solutions v. Federal Insurance*, 2016 WL 7176978 (S.D. N.Y. March 9, 2016). Following discovery, the district court granted summary judgment in favor of Medidata, determining that Medidata had a right to coverage under the Computer Fraud and the Funds Transfer coverage sections.

Computer Fraud Coverage

The Computer Fraud section of the policy provided coverage for "the direct loss of Money, Securities or Property sustained by an Organization resulting from Computer Fraud committed by a Third Party." Computer Fraud was defined as "the unlawful taking or the fraudulently induced transfer of Money, Securities or Property resulting from a Computer Violation." Computer Violation included the fraudulent "entry of Data into … a Computer System" as well as the "change to Data elements or program logic of a Computer System, which is kept in machine readable format … directed against an Organization." Computer System was defined as "a computer and all input, output, processing, storage, off-line media library and communication facilities which are connected to such computer, provided that such computer and facilities are" owned and operated, leased and operated or "utilized by an Organization." *Medidata Solutions v. Federal Insurance*, 2017 WL 3268529.

Federal had denied coverage for Medidata's claim under the Computer Fraud coverage section on the grounds that there had been no Computer Violation because there was no fraudulent entry of data or fraudulent "change to data elements or program logic" of the computer system. Specifically, Federal argued in its motion papers that Medidata's claim was not covered because the fraudster's emails "did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information." In Federal's view, the claim was not covered because the emails themselves did not directly cause the loss—instead, the loss could not have taken place if the Medidata employees did not act on the fraudulent instructions.

In contrast, Medidata contended that the claim was covered under the Computer Fraud section because the perpetrator fraudulently entered and changed data in the computer system. Specifically, Medidata argued that the spoofed address in the "From" field of the emails constituted data entered by the fraudster and that the perpetrator also had to enter a computer code to alter his email address to cause it to look like the email address of Medidata's president.

The district court sided with Medidata, finding that direct hacking was not required by the policy and that "the unambiguous language of the Computer Fraud clause provides coverage for the theft from Medidata." The court explained that "the fraud on Medidata was achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identity. The thief's computer code also changed data from the true email address to Medidata's president's address to achieve the email spoof."

SDNY Relies on Court of Appeals

In so ruling, the Southern District distinguished the Court of Appeals' ruling in *Universal American Corp. v. National Union*, but at the same time relied on the rationale of that opinion. *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, PA*, 25 N.Y.3d 675 (2015). In *Universal American*, the Court of Appeals was presented with a health care company's claim seeking coverage for loss from fraudulent claims for reimbursement entered into the company's computer system by healthcare providers who were authorized to use the system. The Court of Appeals rejected the insured's claim, holding that the policy covered "losses resulting from dishonest entry or change of electronic data or computer program, constituting what the parties agree would be 'hacking' of the computer system." The court concluded that the policy "applies to losses incurred from unauthorized access to [the insured's] computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users." Id.

In *Medidata*, the Southern District explained that Medidata's loss resulted from a violation of the computer system by the type of "deceitful and dishonest access" that the Court of Appeals in *Universal American* had indicated would be covered. The thief's spoofed emails were embedded with a computer code that masked his identify and the true email address, giving him unauthorized access to Medidata's email system. The Southern District held that loss from such unauthorized entry to Medidata's computer system was covered. *Medidata Solutions v. Federal Insurance*, 2017 WL 3268529.

Funds Transfer Coverage

The Southern District also held that Medidata was entitled to coverage under the Funds Transfer Fraud coverage section. The Federal policy defined Funds Transfer Fraud as "fraudulent electronic … instructions … purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent."

Federal denied coverage under the Funds Transfer Fraud section, contending that the Medidata employees voluntarily transferred the funds at issue, and thus the transfer instructions were actually issued by Medidata with knowledge and consent. The Southern District rejected Federal's argument, explaining that "a third party masked themselves as an authorized representative, and directed Medidata's accounts payable employee to initiate the electronic bank transfer … [t]he fact that the accounts payable employee willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction. To the contrary, the validity of the wire transfer 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 Southern District ruling in 'Medidata' does seem to hint at the possibility of an emerging principle—that, generally speaking, computer fraud coverage is intended to apply where the loss results from unauthorized access to the computer system, but not from fraudulent activity by authorized users.

The case is now on appeal to the U.S. Court of Appeals for the Second Circuit.

Looking Forward

The varying details of the fraudulent schemes and the differences in specific policy language require us to approach insurance disputes over payment instruction fraud on a case-by-case basis. However, the Southern District ruling in *Medidata* does seem to hint at the possibility of an emerging principle—that, generally speaking, computer fraud coverage is intended to apply where the loss results from unauthorized access to the computer system, but not from fraudulent activity by authorized users. It remains to be seen whether the Second Circuit will agree and whether this principle can be applied more broadly across different disputes involving varying schemes and policy language.

The insurance industry also appears to be working towards a partial solution on a go-forward basis. Some insurance carriers have begun issuing endorsements that expressly cover loss resulting from payment instruction fraud and related schemes, often subject to sublimits. Where available, these endorsements may provide broader coverage than what is covered under typical commercial crime policies. However, these endorsements are not likely to resolve disputes over claims for coverage filed under already existing crime policy forms.

Schulte Roth&Zabel

Schulte Roth & Zabel LLP
919 Third Avenue, New York, NY 10022
212.756.2000 tel | 212.593.5955 fax | www.srz.com
New York | Washington DC | London