Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Medidata Win Fortifies Policyholders In Digital Fraud Fights

By **Jeff Sistrunk**

Law360, Los Angeles (July 24, 2017, 8:06 PM EDT) -- A New York federal judge recently ruled that a thief's use of emails to trick employees of Medidata into wiring money overseas was a covered incident under the company's computer fraud policy, weakening insurers' arguments that such coverage is meant to apply only to hacking into policyholders' computers.

The computer fraud provision in Medidata Solutions Inc.'s crime policy covered losses that occurred as a result of the "fraudulent entry" or changing of data in the policyholder's computer system. In a Friday decision, U.S. District Judge Andrew L. Carter Jr. held that while Medidata's computers weren't directly hacked by a third party, the provision's requirements were still met because the fraudster used a computer code to alter email messages requesting a funds transfer to make them appear as though they originated from Medidata's president.

Judge Carter pointed out that hacking is "one of the many methods" a thief can use, and concluded that the fraudster's use of deceptive emails to scam Medidata — in what is colloquially referred to as a "social engineering" scheme — is a form of fraudulent entry that falls under the language of the computer fraud provision.

"As the parties are well aware, larceny by trick is still larceny," the judge wrote.

According to Anderson Kill PC shareholder Joshua Gold, Judge Carter's conclusion is a pro-policyholder ruling that is consistent with the policy language, as the computer fraud provision doesn't use the words "hack" or "hacking."

"The gaining of unauthorized access into a computer system can be accomplished in a number of ways: the policyholder can be manipulated into handing over the keys to the kingdom, or a third party can steal the keys to the kingdom by brute force," Gold said. "Under the Medidata court's reasoning, it appears that either scenario would result in coverage."

The chain of events giving rise to the coverage dispute began in September 2014, when an employee in Medidata's accounts payable department received an email from an account purportedly belonging to the company's president that requested a transfer of funds for an acquisition. The message, which was really sent by an unidentified thief, contained the president's picture and email address and copied a fake attorney, according to court papers.

After corresponding with the fake attorney by email and phone and receiving the approval of real high-

level Medidata officers, the employee transferred nearly $4.8 million to a bank account in China, according to the complaint. When it realized it had been duped, Medidata tried unsuccessfully to recover the payment, and the company sued its crime insurer, Federal Insurance Co., after it denied coverage for the loss.

According to attorneys, Judge Carter's Friday decision in the coverage dispute deviated from previous rulings on computer fraud coverage provisions by analyzing, down to a granular level of detail, the means by which the thief defrauded Medidata.

The thief utilized a process called "spoofing," which entailed entering a computer code into the fraudulent emails to trick Medidata's Gmail servers into replacing the displayed email address and profile photo to that of Medidata's president, according to the decision. Federal argued that this scheme didn't equate to computer fraud under Federal's policy because the thief neither accessed nor entered fraudulent information into Medidata's computer system.

In analyzing the computer fraud provision, Judge Carter referred to a 2015 decision by New York's highest court in Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, Pa., which interpreted similar policy language and characterized a "fraudulent entry" as a "violation of the integrity of the computer system through deceitful and dishonest access." Judge Carter found that Federal had applied an overly broad reading of the Universal ruling by focusing on the events that preceded the Gmail server's reception of the fraudulent emails.

"Under this logic, Universal would require that a thief hack into a company's computer system and execute a bank transfer on their own in order to trigger insurance coverage," the judge wrote. "However, this reading of Universal incorrectly limits the coverage of the policy in this case."

From policyholders' perspective, Judge Carter's holding that computer fraud coverage can apply to a variety of deceptive schemes is an important recognition of the ever-evolving toolbox of tactics employed by cybercriminals, attorneys say.

"The court said that an employee being duped into transferring funds via email is functionally the same as the funds being stolen outright," explained Walter Andrews, head of Hunton & Williams LLP's insurance coverage practice.

Critically, the district judge rejected as unpersuasive the Fifth Circuit's decision last year in Apache Corp. v. Great American Insurance Co. that Apache wasn't entitled to computer fraud coverage for a $1.5 million loss the company suffered in a fraudulent scheme that tricked Apache employees into rerouting vendor payments to a sham bank account. The Fifth Circuit held that the loss wasn't covered because a deceitful email sent to Apache by the fraudster was only part of "Apache's multistep, but flawed, process that ended in its making required and authorized, very large invoice payments, but to a fraudulent bank account."

Insurance companies have frequently relied upon the Apache decision in denying coverage for policyholders' losses from social engineering scams. But Judge Carter refused to apply the reasoning in Apache, saying Medidata's employees "only initiated the transfer as a direct cause of" the thief sending the modified emails posing as Medidata's president.

"This is an important point for two reasons," Barnes & Thornburg LLP partner Scott Godes said. "One, the insurance industry has told every court that Apache should be the law of the land, and this court has

rejected that. Two, the court here emphasized that the employees initiated this transfer because they were fooled by the spoofed emails. If a policyholder's employees are deceived into wiring money via a fraudulent email, this decision stands for the position that there is coverage in that situation."

However, Judge Carter's decision by no means gives policyholders a decisive edge in all computer fraud coverage battles, attorneys say. As illustrated by the Medidata and Apache matters, differences in policy language and fraudsters' strategies can lead to drastically different outcomes.

"At the end of the day, the language will vary from policy to policy, and that can lead to different results," said Greg Podolak, managing partner of Saxe Doernberger & Vita PC's southeast office. "Policyholders should know that this is a litigious issue, and carriers will not shy away from taking a hard line to say that policies don't cover employee failings."

Still, attorneys say the ruling provides a road map for future cases and will likely lead courts to more closely scrutinize the means of the fraudulent schemes in forming their conclusions.

"I think there will be more attention paid to how the crime was accomplished from a technical standpoint," Gold said. "Once you get into the technical weeds, I think courts will have a clearer view of the policyholder's grounds for coverage and the insurer's defenses, which should lead to more informed analyses."

To avoid hypertechnical coverage disputes down the road, companies should check the terms of their computer fraud provisions on the front end to ensure the scope of the coverage is clear, attorneys say.

"Going forward, I think companies would be well-advised to look at this coverage and ensure that the policy language is exact," Andrews said. "That would help avoid these kinds of arguments by insurers, and avoid hoping for a judge to reach a decision finding coverage."

The case is Medidata Solutions Inc. v. Federal Insurance Co., case number 1:15-cv-00907, in the U.S. District Court for the Southern District of New York.

--Editing by Katherine Rautenberg and Edrienne Su.
