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 Covered For $4.8M Computer Fraud, Judge Rules

By **Jeff Sistrunk**

Law360, Los Angeles (July 21, 2017, 9:29 PM EDT) -- Medidata Solutions Inc. is entitled to coverage from a Chubb Ltd. unit for a $4.8 million loss it suffered when it was tricked into wiring the money overseas, a New York federal judge ruled on Friday, holding that the incident constituted covered computer fraud under Medidata's crime policy.

The computer fraud provision in Medidata's policy covers losses that occur as a result of the fraudulent entry or changing of data in the policyholder's computer system. 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 unknown fraudster used a computer code to alter a series of email messages to make them appear as though they originated from the company's president.

"The court has reviewed the policy and concludes that, as a matter of law, the unambiguous language of the computer fraud clause provides coverage for the theft from Medidata," Judge Carter wrote.

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 a 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. The fraud was discovered before the employee followed through on a request for an additional transfer of more than $4.8 million when Medidata's president was notified, court papers said.

The perpetrators of the fraud were never identified, and the transferred funds were never recovered, according to the complaint. Medidata filed suit in February 2015 after Federal denied its claim for coverage of the loss under the crime policy's computer fraud, funds transfer fraud and forgery provisions.'

Medidata's coverage dispute with Federal focused largely on the technical details of how the thief composed and sent the fraudulent emails. According to Judge Carter's ruling, at the time of the incident, Medidata employees used a Gmail server for email services. When one employee sent an email to another, the servers would refer to a database of Medidata employee profiles and display the sender's

full name, email address and picture in the message's "from" field, the decision says.

The thief, however, entered a computer code in the fraudulent emails that caused Gmail to change the displayed email address and photo to that of Medidata's president, according to the decision. Federal argued that this scheme didn't equate to computer fraud 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 the case of Universal American Corp. v. National Union Fire Insurance Co., 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." The district judge 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."

Judge Carter noted that hacking is just one of many methods a thief can use to defraud a company, and said the fraudster's approach in Medidata's case is the type of unauthorized, "deceitful and dishonest" access contemplated by the Universal ruling.

The district judge also spurned Federal's argument that the policy's computer fraud coverage doesn't apply because there was no "direct nexus" between the fraudulent emails and the transfer of funds.

The insurer emphasized that the emails themselves didn't result in the transfer; rather, the Medidata employee took multiple steps after receiving the initial deceitful message before carrying out the transfer. But Judge Carter pointed out that the transfer never would have occurred if not for that first email.

"The court finds that Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president," the judge wrote.

Judge Carter further held that the funds transfer fraud provision in Medidata's policy separately provides coverage for the loss. The requirements of that provision, which extends coverage for transfers carried out based on "fraudulent electronic instructions," were clearly fulfilled here, the judge said.

"The 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," Judge Carter wrote. "To the contrary, the validity of the wire transfer depended upon several high level employees' knowledge and consent which was only obtained by trick."

An attorney for Medidata declined comment on the decision, as did a Chubb spokeswoman.

Medidata is represented by Robin L. Cohen, Adam S. Ziffer and Alexander M. Sugzda of McKool Smith PC.

Federal is represented by Christopher M. Kahler, Jeffrey Spiegel, Scott Schmookler and Sara Gronkiewicz-Doran of Gordon & Rees LLP.

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 Joe Phalon.
