Impact of Court Ruling Chubb Unit's Crime Policy Covers 'Spoofed' Wire Transfer

Insurance Journal

In a closely-watched case on insurance coverage in an age of expanding cyber risk, a federal appeals court in New York has upheld a lower court ruling that a commercial crime insurance policy covers wire transfer losses resulting from a spoofing attack.

The ruling is a reminder of how traditional wording in policies continues to be closely scrutinized by insureds for any ties to cyber risk, insurance experts said.

At the same time, the impact of the ruling on future crime insurance coverage may be limited due to facts and policy language specific to this case, according to a lawyer familiar with rulings in this area.

The case Medidata Solutions Inc. v. Federal Insurance Company) before the Second Circuit appeals court involved a crime insurance policy with a computer fraud provision issued by Chubb subsidiary Federal Insurance Co. in June 2014 to Medidata, a clinical trial software firm. The claim involved an increasingly common type of social engineering fraud, an impersonation scam by fraudsters convincing employees to wire funds to external accounts. The policy had a $5 million limit for forgery, funds transfer fraud and computer fraud.

Medidata employees were "spoofed" into wiring $5 million to an account they were led to believe was for an acquisition by a series of fraudulent emails that the fraudsters misrepresented were from an outside attorney and Medidata's own president.

The Federal crime insurance policy defined computer fraud as "the unlawful taking or fraudulently induced transfer of money, securities or property resulting from a computer violation."

Medidata argued that its computer fraud provision should cover its loss because the Federal policy defined a computer violation as any "entry of Data into" or "change to Data elements or program logic of a computer system." The firm argued that the fraudsters entered data when they changed the "From" entry in emails to make it appear they were from real Medidata executives.

Federal Insurance denied the claim, arguing that the email case did not amount to entry of data into or a change to the elements of the Medidata computers. Federal said the policy applies to only hacking-type

intrusions. The insurer also argued that the computer fraud provision was not triggered because the spoof was not the direct cause of the loss since Medidata's own employees made the transfer.

Medidata sued over the claim denial and the U.S. District Court for the Southern District of New York last August awarded Medidata $5.8 million in damages and interest.

Ruling last Friday on an appeal by Federal, the Second Circuit agreed with the district court in finding that the "plain and unambiguous language of the policy" covers the losses incurred by Medidata.

The appeals court found that while no hacking occurred, the fraudsters did insert the spoofing code into Medidata's email system, which the court said is part of the computer system, and they sent messages that were made to look like they were from high officials at Medidata to trick the employees. "Thus the attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system. The attack also made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender. Accordingly, Medidata's losses were covered by the terms of the computer fraud provision," the court found.

The court also rejected Federal's argument that there was no direct link between the loss and the fraudsters' actions. "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," the three-judge ruling said.

The Modern Fraudster: How Courts Are Responding to Social Engineering Fraud

Having decided that Medidata was covered under the computer fraud provision, the Second Circuit court declined to go further and review whether other provisions in the Federal crime policy such as forgery or funds transfer fraud may also apply.

Chubb said it does not comment on litigation matters.

The Medidata case is not the only one that has been closely watched. A similar case with a contrary ruling, American Tooling Center Inc. v. Travelers Casualty & Surety Co. of America, No. 16-12108, 2017 WL 3263356 E.D. Mich. Aug. 1, 2017) is currently on appeal before the Sixth Circuit. In that case, the district court found no crime policy coverage where the Michigan tool and die firm wired $800,000 in funds to a fraudster's account in the belief the account belonged to one of its vendors. The insurer faulted American Tooling for not verifying the bank account with the vendor. In that case, the district court agreed with the insurer that the loss was not a "direct loss" caused by the "use of a computer" and thus the crime policy did not apply. American Tooling has appealed.

The impact of the Medidata ruling is uncertain.

Jonathan Schwartz, a partner with Goldberg Segalla in Chicago, told Insurance Journal the Medidata ruling

“should not greatly affect commercial crime coverage going forward” for two reasons.

First, he noted that the case is unusual in that the hackers infiltrated the insured’s own system in order to spoof emails from the insured’s president. “More often, the hackers purport to be a vendor or outside attorney, which can make detecting the fraud more difficult,” Schwartz said. “All other cases, including American Tooling, involve hacking into a third party’s system to induce the insured into wiring funds to the hackers’ account.”

Second, Schwartz called the ruling an “aberration” because Federal’s policy language is “atypical” of what is in the marketplace.

He also said the order has limited precedential value because it came down as a summary order and not as a full published opinion, although the federal district court decision was published.

Lessons from Case

Policyholder counsel, however, welcomed the Medidata ruling as a signal that insureds may find cyber coverage in existing policies and not just in separate cyber insurance policies.

Joshua Gold, chair of the cyber insurance recovery practice at Anderson Kill and amicus counsel to the consumer group United Policyholders in the Medidata appeal, said the court “rejected arguments that undermine the rationale” for computer fraud insurance coverage.

“This is a reminder that when money, securities or property are stolen by a cyber criminal, policyholders are well advised to consider insurance coverage under more than just dedicated specialty cyber policies and property policies. Crime insurance may be available to cover these types of cyber losses,” Gold said.

The order is also a reminder for insurance industry, according to Erica Davis, senior vice president, JLT Re North America) Inc., who works with carriers on cyber issues.

Davis noted that policy language has evolved and the Federal policy wording from 2014 may not be reflective of norms today, especially related to social engineering and cyber related risk. “Crime policies often address social engineering fraud but the definitions and coverages of this offering differ wildly depending on the carrier, especially in regard to funds transfer,” she told Insurance Journal.

But Davis said there is an important lesson to take from the order about how the growing exposures associated with cyber risk are testing traditional policy language across all lines of business.

“We’re finding this with Crime, Property, D&O and many other lines of business. While the nuances of language evolution may seem slight, this is an example of when the term ‘direct loss’ yielded a significantly different coverage outcome,” Davis said.

Also, wording that “may not have been originally crafted to address elements of cyber risk is now being explored when these events do occur. As an industry, we’ll see this trend continue,” she said. “The best language is specific enough that intent is clear and purposeful – but nimble enough that it stays relevant

as new exposures emerge.”
According to the insurer Beazley, what it calls fraudulent instruction incidents quadrupled in 2017, with policyholders incurring losses ranging from a few thousand dollars up to $3 million. With claims amounts in 2017 averaging $352,000, fraudulent instruction has rapidly become a significant financial threat to many organizations, the insurer said.
The FBI has cited Business Email Compromise BEC) schemes used to intercept and hijack wire transfers as one of the fastest-growing cyber crimes.