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

Travelers' Win Deepens Divide Over Computer Fraud Coverage

By **Jeff Sistrunk**

Law360, Los Angeles (August 2, 2017, 10:17 PM EDT) -- A Michigan federal judge ruled Tuesday that Travelers doesn't have to cover a tool manufacturer's losses from an email-based theft scheme, giving insurers more ammunition to argue that computer fraud insurance doesn't apply to multistep scams and deepening a divide among the nation's courts on the scope of such policies.

The policyholder, American Tooling Center Inc., had been tricked into wiring funds to a phony bank account by thieves who used a process known as "spoofing" to send emails from an address that appeared to belong to a vendor. American Tooling's crime insurance policy with Travelers extended coverage to any "direct loss" that was "directly caused by" the use of a computer, according to court documents.

U.S. District Judge John Corbett O' Meara agreed with the insurer that American Tooling didn't suffer a direct loss attributable to the use of a computer because the company took several steps between the time it received the fraudster's emails and when it wired the funds.

"Given the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that [American Tooling] suffered a 'direct' loss 'directly caused' by the use of any computer," Judge O' Meara wrote.

The ruling was the latest in a string of decisions over the past year interpreting computer fraud coverage provisions for sophisticated email-based "social engineering" schemes, and the results of those cases have been all over the map. Most recently, a New York federal judge found in late July that software company Medidata Solutions Inc. was entitled to computer fraud coverage for a nearly $5 million loss it suffered when it was defrauded in an email scheme similar to the one that targeted American Tooling.

Attorneys who represent insurers say that Judge O' Meara's decision and others rejecting coverage for multifaceted email scams are consistent with the meaning of the phrase "direct loss," which commonly appears in computer fraud provisions. According to White and Williams LLP partner Joshua Mooney, those rulings correctly determined that the use of a computer must be instrumental in a fraudulent scheme, not "merely incidental."

"Some may dispute the reasoning of the courts, but this is not a foreign concept in other insurance contexts," Mooney said. "In a liability case, a claimant who slips down stairs in front of an insured's house does not seek recovery under an auto policy because he happened to use a car to drive to the

house. Just as use of the computer was incidental in this case, use of a car is incidental in my hypothetical."

Meanwhile, attorneys who counsel policyholders opined that the position represented by the Medidata decision is more consistent with insureds' reasonable expectations as to what a computer fraud provision should cover.

"Whether theft is done through a spoofed email or an actual intrusion into the computer system, it shouldn't matter," said Farella Braun & Martel LLP partner Tyler Gerking. "Many of the policies don't say they require an actual intrusion into the insured's computer system. What the Medidata court was getting at was, if you are an insured, and you are defrauded through the use of a computer, you would reasonably expect your computer fraud coverage to cover this sort of loss."

According to court documents, American Tooling had agreed to pay Chinese vendor Shanghai YiFeng Automotive Die Manufacture Co. Inc. at intervals when it hit certain production milestones. Unknown fraudsters posed as representatives of YiFeng and requested that American Tooling wire about $800,000 in payments for real invoices to a bank account controlled by the thieves between March 2015 and May 2015. American Tooling complied, and by the time it discovered the fraud, it was too late to recover the funds, court papers say.

Travelers denied American Tooling's ensuing claim under the computer fraud section of its crime policy on the grounds that the losses were not directly caused by the use of a computer.

American Tooling noted that its policy defined computer fraud as using "any computer" to "fraudulently cause" a money transfer. The company said the scammers indisputably used computers, and while "fraudulently cause" is not defined in the policy, common use of the word "fraud" includes tricking someone into surrendering money.

Judge O' Meara rebuffed the tool manufacturer's arguments, citing to the Fifth Circuit's decision last year in the case of Apache Corp. v. Great American Insurance Co., in which the appellate court found that a similar email fraud scheme wasn't covered under a computer fraud provision.

As in the Apache case, the thieves here used fraudulent emails to impersonate a vendor and deceive the policyholder into wiring funds. But those emails don't constitute the "use of any computer to fraudulently cause a transfer," the district judge held.

"There was no infiltration or 'hacking' of [American Tooling's] computer system," Judge O' Meara wrote. "The emails themselves did not directly cause the transfer of funds; rather, [American Tooling] authorized the transfer based upon the information received in the emails."

The judge further found that the Medidata action was distinguishable because the crime policy at issue in that case did not include the language in American Tooling's policy requiring a direct loss to be "directly caused by" computer fraud.

According to D'Amato & Lynch LLP of counsel David Bergenfeld, the ATC and Apache decisions appropriately recognized that computer fraud coverage should not apply in situations where policyholders had an opportunity to prevent a loss but failed to do so. Judge O'Meara pointed out that American Tooling could have taken steps to verify the authenticity of the bank account purportedly linked to YiFeng but didn't.

"The intervening steps, in essence, gave American Tooling an opportunity to verify these things and protect itself against the loss," Bergenfeld said. "By contrast, if a hacker gains unauthorized access to the insured's computer system and the money is transferred seamlessly, there is no such opportunity."

However, Wargo French LLP partner Raymond Tittmann told Law360 that Judge O' Meara's holding that the email scam didn't lead to a direct loss is "unworkable."

"There is no such thing as a crime that doesn't involve intervening steps," Tittmann said. "The way the court has interpreted 'direct' eviscerates the computer fraud coverage in a crime policy."

Cohen & Grigsby PC partner Roberta Anderson said that in her experience, companies expect that losses to social engineering schemes will fit within the scope of their crime policies' computer fraud coverage. Any decisions to the contrary, therefore, contravene those expectations, she said.

"The fake and fraudulent request that the company receives is virtually always accomplished through the use of a computer," Anderson said.

But Wiley Rein LLP partner Mary Borja said that the ubiquity of computers in businesses' operations is the very reason that limitations on computer fraud coverage are necessary.

"In these types of schemes, a computer is being used, but in modern American business, computers are used all day long," Borja said. "As a result, the American Tooling and Apache courts found that the use of a computer as a part of the scheme, by itself, doesn't satisfy the policy language."

Crowell & Moring LLP partner Laura Foggan said Judge O' Meara hit the nail on the head when he cited to another influential computer fraud coverage case out of the Ninth Circuit, Pestmaster Services Inc. v. Travelers.

In Pestmaster, the appellate court emphasized that because computers are used in nearly every business transaction, interpreting a computer fraud provision to cover "all transfers that involve both a computer and fraud at some point in the transaction" would convert a crime policy into a "general fraud" policy.

"I think that is really the key point: There are important limits on computer crime coverage that have to be given effect or else these policies would be read to respond to virtually every business loss of funds," Foggan said.

The Medidata decision and several others finding that computer fraud provisions encompass losses tied to social engineering schemes — most notably, a Georgia federal court's September decision in favor of an information technology company that lost $1.7 million to such a scam — provide road maps for policyholders to fight for coverage in similar circumstances. However, the pro-insurer decisions in the American Tooling and Apache matters highlight the importance of companies negotiating the clearest computer fraud language possible upfront, according to attorneys.

It may be possible to narrow or delete the "direct loss" language or to obtain additional coverage specifically designed for social engineering losses, attorneys say.

"Some courts are making some very technical distinctions in the policy language," Gerking said. "From a

practical standpoint, this goes to show that companies buying crime coverage ought to be carefully looking at the policy they are getting in close consultation with their insurance broker and coverage counsel."

--Editing by Christine Chun and Aaron Pelc.
