THOMSON REUTERS

Westlaw®

Computer fraud coverage and email hacks

By John K. DiMugno, Esq., *Insurance Research Group*

NOVEMBER 9, 2018

In recent years, crime insurers have received claims for theft losses that were unheard of before the advent of our high-tech, global economy, where business transactions occur online without any personal contact between the parties.

We've all heard stories of direct computer hacks to steal data or money from a business electronically without contacting staff. These hacks result in a direct loss caused by the use of a computer, and so are covered under the computer fraud provisions of the business's crime insurance policy.

But improvements in business firewalls and anti-hacking software have caused scammers to change tactics. Rather than gain direct electronic access to a business's bank accounts, they hack into its email servers to manipulate employees into doing what the hackers can no longer do directly.

Known variously as spoofing, business email compromise, social engineering or, my favorite, "fake president" fraud, this new tactic entails commandeering a high-level executive's email account. The scammer then uses the executive's email address and online identity to instruct an employee to transfer funds into a bank account controlled by the scammer.

Although the loss resulting from these spoofing attacks is identical to the loss resulting from a direct hack, insurers have consistently denied coverage for spoofing claims on the ground they do not involve a direct loss caused by a computer.

Insurers have argued with some success that the presence of authorized employee actions in the causal chain of events vitiates the causal connection between the use of the computer and the loss of funds.

A CHANGE OF DIRECTION?

Both *American Tooling Center Inc. v. Travelers Casualty and Surety Co. of America*, 895 F.3d 455 (6th Cir. 2018), and *Medidata Solutions Inc. v. Federal Insurance Co.*, 729 F. App'x 117 (2d Cir. 2018), reject the insurers' argument.

They hold that a crime policy's computer fraud coverage is not limited to direct hacking, but also applies when email spoofing causes the policyholder's employee to transfer funds to a scammer impersonating an executive or vendor.

American Tooling

The 6th U.S. Circuit Court of Appeals' decision in *American Tooling* is particularly significant because it overrules a federal district court decision that insurers frequently relied on to deny coverage.

In *American Tooling,* the insured's treasurer sent a vendor's employee an email requesting all outstanding invoices.

An unidentified third-party hacker intercepted this email and, impersonating the vendor's employee, instructed the treasurer to wire the insured's payments to an account the hacker controlled. The treasurer did so, transferring over $800,000 via several transactions.

Only when the real vendor demanded payment did the insured realize it was the victim of a scam. The insured paid the vendor 50 percent of the outstanding debt, and the vendor agreed payment of the remaining 50 percent would be contingent on an insurance claim under its crime policy.

The insured sought coverage under the computer fraud provisions of its crime policy with Travelers. Travelers denied coverage, asserting that the insured did not suffer a "direct loss," the case did not involve "computer fraud," and the loss was not "directly caused by computer fraud."

The 6th U.S. Circuit Court of Appeals' decision in *American Tooling* is particularly significant because it overrules a federal district court decision that insurers frequently relied on to deny coverage.

The U.S District Court for the Eastern District of Michigan granted summary judgment to Travelers, but the 6th Circuit reversed and granted summary judgment in favor of the insured.

Applying Michigan law, the 6th Circuit first rejected the District Court's holding that the insured did not suffer a direct loss. The District Court had reasoned that the loss did not occur when the insured wired funds to the scammer. It said the loss occurred later, when the insured agreed to pay the vendor at least half of the money owed.

Disagreeing with the District Court, the 6th Circuit pointed to Michigan appellate decisions construing the word "direct" to mean proximate or immediate, as distinct from remote or incidental. The appeals court reasoned that the insured suffered a direct loss when it transferred funds to the hacker.

The 6th Circuit flatly rejected the insurer's argument that the scammer's conduct did not constitute "computer fraud," which the policy defined as the use of a computer to fraudulently cause a transfer of money to a person or place outside the company.

Travelers had argued that the definition requires a computer to "fraudulently cause the transfer," and that it was not sufficient to simply use a computer to fraudulently induce an authorized employee's transfer of funds.

The court expressly refused to limit coverage to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer." If the insurer had wanted to limit coverage in this manner, the court observed, it should have done so by using unambiguous policy language.

Is so ruling, the court distinguished an unpublished decision from the 9th U.S. Circuit Court of Appeals, *Pestmaster Services Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332 (9th Cir. 2016). In *Pestmaster*, the insured had outsourced its payroll services and granted its vendor electronic access to its bank account. The vendor was authorized to transfer funds out of Pestmaster's bank account into its own account to pay Pestmaster's payroll taxes.

The fraud occurred when the vendor kept the money instead of paying the taxes. Thus, everything occurring using the computer was legitimate, and the fraudulent conduct occurred without the use of a computer. By contrast, in *American Tooling*, the scammer used a computer to send American Tooling spoofed emails that caused the company to transfer the money.

Medidata Solutions

A week before the 6th Circuit issued its opinion in the *American Tooling* case, the 2nd U.S. Circuit Court of Appeals reached a similar result in *Medidata*.

In *Medidata*, employees of the policyholder company transferred more than $5 million because of fraudulent email instructions that appeared to come from Medidata's president. The scammers went to great lengths to impersonate the president, including putting his email address and picture in the "From" field.

In affirming the lower court's finding of coverage, the 2nd Circuit, applying New York law, rejected the insurer's contention that the policy's direct-loss requirement limited coverage to direct-hacking-type intrusions and did not include losses that occur when the policyholder's own employees initiate the transfer.

The court interpreted "direct loss" to mean "a proximate cause" and concluded that the fraudulent email impersonating the company's president proximately caused the loss. Although authorized Medidata employees themselves transferred the funds, that did not, in the court's view, interrupt the chain of causation between the initial fraud and the ultimate loss.

The court rejected the insurer's argument that the spoofing attack did not fall within the grant of coverage for losses stemming from any "'entry of data into' or 'change to data elements or program logic of' a computer system."

"While Medidata concedes that no hacking occurred," the court said, "the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system."

"The attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system," the court said. "The attack ... made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender."

CONCLUSION

Perhaps the 2nd Circuit discussed the technical aspects of the intrusion into the policyholder's email system so extensively because the policy required "fraudulent entry of data into" or "change to data elements or program logic of" a computer system. In contrast to Medidata's policy, some policies require only some "use" of a computer to fraudulently transfer money.

At least one court, the 5th U.S. Circuit Court of Appeals in *Apache Corp. v. Great American Insurance Co.*, 662 F. App'x 252 (5th Cir. 2016) (per curiam), has held that the mere sending of an email by a criminal is not the type of "usage" that could trigger coverage.

"To interpret the computer fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would ... convert the computer fraud provision to one for general fraud," the *Apache* court said.

The 2nd Circuit's decision in *Medidata* provides a blueprint for policyholders to overcome this defense by presenting evidence on the technical details of the criminal's scheme.

This article first appeared in the November 9, 2018, edition of Westlaw Journal Insurance Coverage.

ABOUT THE AUTHOR

John K. DiMugno of **Insurance Research Group** in Cameron, California, has testified as an expert witness on a wide variety of insurance coverage and bad-faith issues for both policyholders and insurance companies. He is the author of numerous articles and is a co-author of three insurance law treatises published by Thomson Reuters. For a complete list of his publications and presentations, visit dimugnolaw.com.