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

Apache Ruling Narrows Reach Of Digital Fraud Coverage

By **Jeff Sistrunk**

Law360, Los Angeles (October 20, 2016, 7:10 PM EDT) -- The Fifth Circuit's ruling Wednesday that Apache Corp. isn't covered for losses stemming from a fraudulent scheme that caused it to reroute vendor payments to a phony account curtails the use of computer fraud insurance to cover complex, multistep scams, requiring that an act of computer-based deception directly cause the loss, experts say.

Reversing a Texas federal court's decision, an appellate panel agreed with Great American Insurance Co. that the oil and gas exploration company's losses weren't covered because an email to Apache containing instructions to change a vendor's payment information didn't directly cause a series of fraudulent transfers. The computer fraud provision in Apache's commercial crime policy with GAIC extended coverage for losses "resulting directly from the use of any computer to fraudulently cause a transfer."

The panel determined that the fraudulent email was just one step in an intricate scheme that ultimately led Apache employees to authorize legitimate transfers, albeit to a bogus bank account.

"The email was part of the scheme, but the email was merely incidental to the occurrence of the authorized transfer of money," the panel wrote. "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."

According to experts, the decision will curtail coverage under commercial crime policies for many so-called "social engineering" scams in which a criminal manipulates a company's employees into transferring money into a fraudulent account. Such schemes often involve a combination of deceptive emails, phone calls and even written communications.

Attorneys representing policyholders say that the Fifth Circuit's reasoning may unfairly foreclose coverage for losses that a company would expect to fall under a typical computer fraud policy provision.

"It was unfortunate the court minimized the role of the electronic communication in perpetrating the fraud, saying that it was incidental to the overall crime," said Anderson Kill PC shareholder Joshua Gold. "It seems to me that this event was exactly what the policyholder would have expected the policy to cover — theft perpetrated via computer fraud."

On the other hand, attorneys who represent insurance carriers said that the Fifth Circuit panel properly limited the scope of GAIC's coverage in accordance with the policy language.

"In Apache, the Fifth Circuit in essence rejected a syllogistic fallacy akin to 'all tigers have stripes; all tigers are mammals; therefore, all mammals must have stripes,'" said Joshua Mooney, co-chair of White and Williams LLP'scyber law and data protection group. "The syllogistic fallacy was: Apache used a computer. Apache suffered a fraud. Therefore, the fraud was from Apache's use of a computer. Coverage can't work that way."

The coverage dispute stemmed from a March 2013 incident that began when an accounts payable employee with Apache's North Seas division received a call from an individual who falsely claimed to be employed by one of the company's vendors, Petrofac Facilities Management Ltd.

The imposter told the Apache employee that Petrofac was transitioning its accounts from Royal Bank of Scotland to another bank and wanted to provide Apache with the company's new account information for future wire payments, according to court documents. After the fraudster sent an email containing a written request on Petrofac letterhead and Apache employees confirmed the change over the phone with a person posing as a real Petrofac representative, Apache sent $7 million in Petrofac invoice payments to a bogus account, court papers said.

Apache was ultimately able to recover all but $2.4 million of the lost money, but GAIC denied the company's claim for coverage under its commercial crime policy, saying the scheme's success hinged on the phone call to the individual posing as a Petrofac employee rather than computer fraud.

U.S. District Judge Alfred H. Bennett rejected GAIC's contention and granted Apache summary judgment in August 2015, finding that, despite the steps that preceded and followed Apache employees' reception of the fraudster's email, the email was still a "substantial factor" in the loss. The judge awarded Apache just under $1.5 million after taking the policy's deductible and other considerations into account.

The Fifth Circuit panel, however, found that Judge Bennett had erred, saying the fact that the scam involved an email communication didn't necessarily render it computer fraud. The panel pointed out that few, if any, modern fraudulent schemes don't involve some form of computer-facilitated communication.

"Arguably, Apache invited the computer use at issue, through which it now seeks shelter under its policy, even though the computer use was but one step in Apache's multistep, but flawed, process that ended in its making required and authorized, very large invoice payments, but to a fraudulent bank account," the panel wrote.

Mooney said that the Fifth Circuit's decision was appropriate given the ubiquity of computerized communication utilizing everything from personal computers to cellphones.

"Given the wide use of computers in almost every facet of our lives, the Fifth Circuit clearly feared that to allow use of email to implicate coverage for computer fraud would transform 'computer fraud' coverage into coverage for any fraud," Mooney said.

David Bergenfeld of D'Amato & Lynch LLP, who also represents insurers, noted that Texas courts and the Fifth Circuit have a history of holding that the "resulting directly" language at issue in the case requires a "very close nexus between the insured peril and the loss."

"The Fifth Circuit in its decision appears to have analyzed the case from the point in time when the money was actually sent out from the insured. The insured authorized the wire transfer based upon legitimate invoices," Bergenfeld said. "Therefore, the Fifth Circuit concluded that the email did not cause the loss."

Given the relative scarcity of appellate-level case law interpreting computer fraud policy provisions, the Fifth Circuit's decision could have a significant impact both inside and outside of the circuit, according to attorneys.

"As there is not a tremendous amount of case law in this area, courts will continue to rely upon and analyze cases from courts across the country as the Fifth Circuit did in its decision," Bergenfeld said. "Further, the Apache case will reinforce the 'direct means direct' line of cases for interpreting cybercrime policies. In other words, insurance coverage under similar cybercrime policies will be narrower."

Policyholder attorneys say the ruling could have troubling implications for insureds due to its conclusion that computer fraud coverage doesn't apply if a criminal carries out a multifaceted scheme that includes tactics beyond a deceptive email or direct hacking into a network.

"It is a strange ruling in that, because a criminal has a more elaborate scheme to steal — [for example] starting with impersonating a business partner through computer messages and then using the telephone — this can somehow negate your computer fraud coverage," Gold said.

However, the decision isn't a death knell for computer fraud coverage for all types of sophisticated criminal schemes, attorneys say. In one recent decision, for instance, the Eighth Circuit **found** that a Minnesota bank was entitled to coverage under a BancInsure financial institution bond for a loss due to a fraudulent transfer carried out by a hacker. The appeals court held that, although bank employees negligently failed to secure a computer network, the hacker's criminal acts were still the main cause of the loss.

The Eighth Circuit's ruling suggests that coverage may still exist under computer fraud provisions in cases where criminals directly carry out unauthorized transfers or other fraudulent activities, according to attorneys.

"In that case, there was an unauthorized transfer of funds effected directly by a hacker, rather than by an authorized user that had been duped, and that's why I think the Eighth Circuit found coverage," said John C. Pitblado, aCarlton Fields Jorden Burt PA shareholder and insurance litigation attorney.

The surge in litigation over the scope of computer fraud insurance may lead insurers to rewrite the language in such provisions to clearly limit coverage to instances of hacking, attorneys say. In addition, some carriers have already started rolling out policy riders at an additional cost that directly address complex scams like the one targeting Apache.

"We [may] see insurers going back to the drawing board on these riders and changing these computer fraud provisions to make clear that they are meant to only apply to hacking-type incidents ... and we're already seeing new riders designed to address [business email compromise] and similar schemes explicitly," Pitblado said.

Policyholders may also be able to secure coverage for social engineering schemes via specialized cyber coverage, attorneys say.

"Cybersecurity products really offer a broad range of protection against these types of risks," Mooney said. "Computer fraud policies are not intended to cover the array of risks that cyber policies are designed to cover."

Apache is represented by Patrick W. Mizell and Deborah Carleton Milner of Vinson & Elkins LLP and David H. Brown of Brown & Lewis LLP.

Great American is represented by F. Joseph Nealon and Michael A. Graziano of Eckert Seamans Cherin & Mellott LLC and William G. Winget, Harris B. Katz, Gary T. Stevens Jr., Eric W. Swartz and Martin S. Schexnayder ofWinget Spadafora & Schwartzberg LLP.

The case is Apache Corp. v. Great American Insurance Co., case number 15-20499, in the U.S. Court of Appeals for the Fifth Circuit.

--Editing by Philip Shea and Katherine Rautenberg.
