THOMSON REUTERS
Westlaw®

Computer fraud insurance in the cyberage

By Robert A. Stines, Esq., *Freeborn & Peters**

JULY 13, 2018

Electronic communications are ubiquitous in modern society. Companies now rely on the internet, email, text messages, social media and artificial intelligence chatbots to compete.

The rise of electronic communications presents a major challenge to companies because, to the extent fraud is perpetuated through the exchange of information, many fraudulent schemes involve some form of computer-facilitated communication. There are many reports of criminals exploiting society's reliance on electronic communication for financial gain (e.g., phishing, spoofing and social engineering).

As companies fall victim to fraud through the use of computers, they may seek coverage under computer fraud or computer crime provisions in insurance policies (collectively, computer fraud provisions).

The Insurance Services Office Inc. has two forms that provide coverage for computer fraud or computer crime. These forms specify that the loss must result *directly* from the use of a computer. Some insurance companies have adopted language similar to that used on the ISO forms.

Since 2016, there have been some important cases interpreting computer fraud provisions. The outcome of those cases has surprised many and left some to think the name "computer fraud insurance" is misleading.

This analysis will discuss how courts have interpreted computer fraud provisions, identify the common themes in those decisions, and consider possible implications for applying those themes to emerging technologies.

CASES INTERPRETING COMPUTER FRAUD PROVISIONS

Pestmaster Services v. Travelers Casualty & Surety Co.

In 2016 the 9th U.S. Circuit Court of Appeals affirmed a district court's conclusion that there was no coverage under a computer fraud provision.[1]

In 2009, Pestmaster hired a payroll contractor, Priority 1 Resource Group, to withhold and submit the company's payroll taxes. To allow Priority 1 to perform the services, Pestmaster executed an automated clearing house authorization that allowed Priority 1 to automatically transfer funds from Pestmaster's bank account to Priority 1's bank account.

Priority 1 used Pestmaster's funds to pay Priority 1's own expenses, leaving Pestmaster on the hook to the IRS for payroll taxes.

Pestmaster filed a claim with Travelers Casualty & Surety Co. America under a Crime+Wrap policy that included a provision covering losses resulting from computer fraud.

The computer fraud provision provided coverage for "direct loss of, or your direct loss from damage to, money, securities and other property directly caused by computer fraud." The policy defined "computer fraud" as the use of any computer to fraudulently cause a transfer.

The District Court reasoned that computer fraud under the policy occurs when someone either "hacks" or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer fraudulently to cause a transfer of funds.[2]

> If there were several steps between the fraudulent access or communication and the loss, then the insured had opportunity to discover the fraud and avoid the loss.

It was undisputed that Pestmaster authorized Priority 1 to initiate ACH transfers from its account to Priority 1's account so that Priority 1 could pay Pestmaster's payroll and payroll taxes.

The Court found that Priority 1's fraudulent conduct occurred only after the authorized transfer to Priority 1's account had been completed pursuant to its agreement with Pestmaster.

Based on the undisputed facts, the court determined that Pestmaster's claimed losses did not "flow immediately" and "directly" from Priority 1's use of a computer. Rather, Pestmaster's losses occurred after Priority 1 made the authorized transfer of funds — when Priority 1 used those funds to pay its own obligations instead of Pestmaster's federal payroll taxes.

In affirming the District Court, the 9th Circuit noted that almost every business transaction involves computers. Therefore, it said, reading the computer fraud provision to cover all transactions that at some point involve both a computer and fraud would convert the computer fraud provision into general fraud insurance.

Apache Corp. v. Great America Insurance Co.

In 2016 the 5th U.S. Circuit Court of Appeals agreed with Great American Insurance Co. that Apache Corp.'s loss of $1.5 million was not covered under a computer fraud provision.[3]

In 2013 an Apache employee in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, a vendor for Apache. The caller instructed the Apache employee to change the bank account information for its payments to Petrofac.

The employee replied that the change request could not be processed without a formal request on Petrofac letterhead.

A week later, Apache's accounts-payable department received an email from an address at petrofacltd.com. But Petrofac's authentic email domain name is petrofac.com. The fraudsters created petrofacltd.com to send the fraudulent email.

The email advised Apache that Petrofac's account details were recently changed and directed Apache to make payment to the new account. A signed letter on Petrofac letterhead was attached to the email.

In response to the email, an Apache employee called the telephone number provided on the letterhead to verify the request and confirm the authenticity of the change request. Next, a different Apache employee approved and implemented the change.

A week later, Apache transferred funds for payment of Petrofac's invoices to the new bank account.

Within one month, Apache received notification from Petrofac that it had not received payment.

Apache submitted a claim to Great American asserting coverage under the computer fraud provision, which states:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises:
>
> a. to a person (other than a messenger) outside those premises; or b. to a place outside those premises.

In its denial letter, Great American advised Apache that its "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."

The 5th Circuit acknowledged that the email was part of the scheme, but it concluded the email was merely incidental to the occurrence of the authorized transfer of money.

The court outlined all the steps that occurred between Apache's receipt of the email and its authorized funds transfer. Those steps included an Apache employee calling the telephone number on the fraudulent Petrofac letterhead instead of calling a pre-existing number for the vendor, and another Apache employee approving and implementing the change, which resulted in the authorized transfer of funds to a fraudulent account.

The court opined that reducing the multistep process to its simplest form, Apache made the transfers in order to pay legitimate invoices — and not because of fraudulent information.

American Tooling Center v. Travelers Casualty & Surety Co.

Relying in part on *Apache*, a federal judge in Michigan ruled in August 2017 that Travelers was not obligated to cover American Tooling Center Inc.'s losses resulting from a fraudulent email-based scheme.[4]

American Tooling outsourced some of its work to overseas manufacturing companies, one of which was YiFeng Automotive Die Manufacture Co. Ltd. American Tooling typically issued purchase orders to YiFeng, and YiFeng performed the work.

> Computer fraud provisions that require direct loss from computer use are not intended to address most of the fraud that occurs through the use of computers.

American Tooling paid YiFeng in stages when specific production milestones were reached.

To receive payment, YiFeng emailed an invoice for each milestone. After verifying the milestones were met, American Tooling initiated wire transfers from its bank account to YiFeng's bank account.

In 2015 American Tooling emailed YiFeng requesting copies of all outstanding invoices. But the response American Tooling received came from a fraudster using the domain yifeng-rnould, which is strikingly similar to the correct domain, yifeng-mould.com.

The fraudster, feigning association with YiFeng, instructed American Tooling to send payment for several legitimate outstanding invoices to a new bank account. Without verifying the new banking instructions, American Tooling wired roughly $800,000 to a bank account that the fraudsters controlled.

American Tooling sought coverage for the loss from Travelers under a computer fraud provision. Similar to the provisions in *Apache* and *Pestmaster*, the provision covered American Tooling's "direct loss of, or direct loss from damage to, money ... directly caused by computer fraud."

Travelers contended that American Tooling did not suffer a "direct loss" that was "directly caused" by "the use of any computer." Instead, Travelers argued, American Tooling

received emails that were fraudulently spoofed to appear as though sent by YiFeng, and in response, American Tooling authorized payment to the bank account specified in the fraudulent emails after verifying that certain production milestones had been met.

The court agreed and concluded that the intervening events between American Tooling's receipt of the fraudulent emails and its transfer of funds precluded a finding of "direct" loss "directly caused" by the use of any computer.

Interactive Communications v. Great American Insurance Co.

More recently, the 11th U.S. Circuit Court of Appeals affirmed a lower court's grant of summary judgment in favor of Great American Insurance Co.[5]

Interactive Communications International Inc. was in the business of selling "chits" — each of which had a specific monetary value — to consumers who, after purchasing a chit at a retailer, could simply call InComm to redeem the chit and have its value transferred to a debit card.

When calling InComm's phone number, the consumer was connected to an interactive voice response computer system. Fraudsters manipulated a glitch in InComm's IVR system that enabled multiple redemptions of a single chit. This manipulation resulted in an $11.4 million loss.

Similar to the provision in *Apache*, Great American's computer fraud provision provided coverage for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises.

Interestingly, the District Court found the fraud was accomplished through the use of phones rather than the use of a computer.

The 11th Circuit disagreed, noting the IVR system was comprised of eight computers that processed transaction requests from cardholders, so the fraudsters' use of phones to manipulate the IVR system necessarily involved computers.

The 11th Circuit agreed with the District Court that InComm's loss did not "result directly" from the use of the IVR system. To explain its reasoning, the court both explored the meaning of the phrase "resulting directly" and examined when InComm's loss occurred.

The court broke down the fraud against InComm into four distinct steps:

- Step 1: The fraudsters manipulate the IVR system to enable duplicate chit redemption.
- Step 2: After processing the redemption call through the IVR system, InComm transfers money to the bank that issues the debit card.
- Step 3: A debit card user (the fraudster) makes a purchase from a merchant, incurring debt to be paid from the InComm-earmarked bank account.
- Step 4: The bank transfers money from the account to the merchant to cover the purchase made by the debit card user (the fraudster).

InComm argued that its loss occurred at Step 2, which resulted directly from the Step 1 fraud. But the court concluded that InComm still had some control over the funds after it transferred the money to the bank because it could prevent the loss by intervening to halt the disbursement of money from the bank to the merchants.

The court noted that the chain of causation involved intervening acts and actors between Step 1 and Step 4, and it determined that InComm's loss actually occurred at Step 4, when the bank disbursed the money from the InComm-earmarked account to pay merchants for purchases made by the cardholders.

Ultimately, the court held that InComm's loss did not result directly from the fraudulent use of its IVR computer system; therefore, it decided that the loss was not covered.

AUTHORIZATION AND STEPS

These cases clearly indicate that the computer fraud provisions at issue were intended for situations in which an individual uses a computer to gain access to an insured's internal computer system and then uses that access to transfer funds from the insured's premises.

As the court in *Pestmaster* noted, these provisions were designed to cover hacking[6] of computers that results directly in the fraudulent transfer of funds or property. None of the cases discussed above involved a classic hack. Instead, in each of them the fraudsters relied on human error or oversight.

In deciding whether there was a loss resulting directly from the use of a computer, these cases hinge on the answers to two key questions:

- Did the insured, at any point, authorize the transfer?
- Were there any intervening steps between the initial fraudulent communication and the loss?

If the insured authorized the fraudulent transfer, the loss can be chalked up to human error rather than the manipulation of computer systems. Similarly, if there were several steps between the fraudulent access or communication and the loss, then the insured had opportunity to discover the fraud and avoid the loss.

HUMAN INTERVENTION OR INTERRUPTION

Despite their focus on whether the victim authorized the fraudulent transfer and the number of steps included in the

fraudulent process, the courts seem to suggest that these losses were really caused by human error or gullibility.

In *Pestmaster*, one human at Pestmaster trusted another human at Priority 1 to comply with the company's contractual obligations, but that trust was misplaced.

In *Apache* and *American Tooling*, if humans had properly investigated or verified the account changes, then the losses likely would have been avoided.

In *InComm*, the court indicated that between the many steps leading to the loss, InComm had the power to intervene and stop the transfer of the funds.

If a human was, or should have been, involved in the process either by providing authorization or conducting an investigation, then courts will likely conclude that the loss did not result directly from the use of a computer.

As the court in *InComm* explained, "one thing results 'directly' from another if it follows straightaway, immediately, and without any intervention or interruption." The decision suggests there cannot be a direct loss from computer use if there was actual or even possible human intervention or interruption.

CYBERCRIMES AND EMERGING TECHNOLOGY

Computer fraud provisions that require direct loss from computer use are not intended to address most of the fraud that occurs through the use of computers.

The sad truth is that scammers and fraudsters do not need to gain unauthorized access to computer systems to steal money. In fact, there are very few reports of hackers gaining access to a company's internal computer system and transferring funds from the company's premises.

Instead, hackers gain access to computer systems for the purpose of stealing personally identifiable information, such as Social Security numbers, birth dates, email addresses, and passwords (e.g., Equifax, Home Depot, Target, Yahoo).

Hackers then use the PII to impersonate consumers online by using their credit cards, accessing their bank accounts and applying for loans.

There are also reports of hackers gaining access to steal confidential information or trade secrets.[7]

Additionally, hackers gain access to computer systems to install ransomware to elicit the payment of money.[8]

Most computer fraud provisions will not apply to these forms of cybercrimes.

If the possibility of human intervention reduces the likelihood of coverage under these provisions, it will be interesting to see how artificial intelligence and automation will impact future insurance claims.

Companies are beginning to understand and appreciate the benefits of using artificial intelligence and automation to handle customer relations and repetitive, time-consuming tasks.[9]

Anyone who has used a smart speaker to purchase items online will understand that human interaction is becoming unnecessary in e-commerce. In the future, it is highly likely that companies in the retail or banking industries will rely on automation, artificial intelligence and voice-driven technology to handle many routine tasks.

It is probably possible to eliminate all human intervention or interaction in the steps outlined in *InComm*. There are already demonstrations of artificial intelligence and virtual assistants making calls on behalf of humans.[10]

It will be possible for fraudsters to program artificial intelligence to interact with computers such as the IVR system used in *InComm*, meaning artificial intelligence would handle the entire process leading to the fraudulent transfer of funds. Under those facts, would the court still find that the loss did not directly result from the use of computers?

CONCLUSION

As courts continue to agree with insurance companies denying coverage, the message is clear: If insurance companies intended computer fraud provisions to cover all transfers that in some way involve both a computer and fraud, then almost every fraud in the cyberage would be covered. Insurance companies plainly cannot afford such an interpretation.

It will be interesting to see if insurance companies tighten their language to cover only the classic hack, or if new insurance products come to market that will cover the many permutations of fraud that occur through the use of computers and emerging technologies.

For certain, the implementation and utilization of emerging technologies in modern business will strain the interpretation of insurance policies and force courts to decide cases in uncharted territories.[11]

NOTES

[1] *Pestmaster Servs. Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332 (9th Cir. 2016).

[2] *Pestmaster Servs. Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 13-cv-5039, 2014 WL 3844627 (C.D. Cal. July 17, 2014).

[3] *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016).

[4] *Am. Tooling Ctr. Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 16-cv-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).

[5] *Interactive Commc'ns Int'l Inc. v. Great Am. Ins. Co.*, No. 17-11712, 2018 WL 2149769 (11th Cir. May 10. 2018).

[6] To surreptitiously break into the computer, network, servers or database of another person or organization. *Hack*, Black's Law Dictionary (10th ed. 2014).

[7] Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://bit.ly/1pySTOP.

[8] Grace Johansson, *Cyber-attack shuts down US Regional Hospital's online system*, SC MEDIA (Jan. 16, 2018), https://bit.ly/2B92frc.

[9] Patricia Carlin, *Understanding the Role of Artificial Intelligence in Payments*, FORBES.COM (May 20, 2018), https://bit.ly/2tFlffe.

[10] Michael Oliveira, *Google's seamless personal assistant sparks concerns about the future of AI*, TORONTO STAR, May 12, 2018, https://bit.ly/2yOb1iD.

[11] This article is not intended to provide an exhaustive risk analysis of computer fraud or computer crime provisions. The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

This article first appeared in the July 13, 2018, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Robert A. Stines is a partner in the Tampa, Florida, office of **Freeborn & Peters**. A member of the firm's litigation practice group and emerging technologies industry Team, Stines is a trial lawyer whose practice is focused on business litigation, commercial disputes and professional liability defense. He can be reached at rstines@freeborn.com.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.