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

5 Fraud Insurance Decisions Sure To Shape 2019

By **Patricia Carreiro** (January 18, 2019, 12:46 PM EST)

Patricia Carreiro

2018 brought with it a slew of much anticipated coverage decisions. Here are a few federal appellate court decisions sure to shape case law going forward and some things to watch for in 2019. Going into 2018, we knew courts were divided on computer fraud insurance coverage for phishing scams.[1] In 2018, the split continued, with federal appellate courts slightly, but still not universally, favoring coverage for phishing scams. Oversimplifying those decisions into a simple coverage versus no-coverage distinction without considering the courts' underlying bases, however, is a mistake. Each policy's language, the circumstances surrounding the loss, and the governing law all played significant roles.

Metadata Solutions v. Federal Insurance. Co.[2]

The background facts of this summary order are all too familiar: an employee tricked into transferring money by a spoofed email pretending to be from the company's president. The insured's crime policy covered "a direct loss of money, securities or property" due to computer fraud or funds transfer fraud committed by a third party. The policy definitions played a large role in finding coverage in this case, defining computer fraud as encompassing the fraudulent entry of data into or the changing of data in the policyholder's computer system, while its definition of funds transfer fraud included transfers carried out based on "fraudulent instructions." The lower court found coverage based on the fraudster's altering of computer code to make the email messages appear to be from the company's president and, even apart from the first basis, because it read the funds transfer fraud provision as providing coverage for the loss. While the insurer argued against coverage based on the policy's requiring a direct, unauthorized change to the insured's systems and because the email wasn't the direct cause of loss (it was followed by a phone call and approvals and actions by multiple employees), the Second Circuit disagreed, affirming the lower court's coverage finding.

American Tooling Center v. Travelers[3]

In American Tooling, a fraudster, posing as a supplier's representative, tricked a company into wiring payment for real invoices into the fraudster's account. The crime policy covered "direct loss" of funds "directly caused by computer fraud," which was defined as "the use of any computer to fraudulently cause a transfer of money." The lower court, relying heavily on Sixth Circuit precedent limiting "direct" to immediate with no intervening events, initially found against coverage based on the loss not being directly attributable to the use of a computer. A three-judge panel reversed, and the Sixth Circuit declined a motion for an en banc rehearing. The Sixth Circuit in American Tooling specifically distinguished another notable 2018 decision, which also addressed the necessary connection between event and loss: Interactive Communications Int'l Inc. v. Great American Insurance Co.[4]

Interactive Communications International Inc. v. Great American Insurance Co.

Fraudsters utilized a glitch in InComm's system to repeatedly redeem the same debit card value over the phone before InComm's systems realized that the card had already been previously redeemed. The lower court found against coverage based on the fraudster's use of phones to redeem the cards being outside the policy's coverage. The Eleventh Circuit disagreed, but still found no coverage based on the losses being "temporally remote" rather than "direct" as needed

found no coverage based on the losses being "temporally remote," rather than "direct," as needed for coverage. Applying Georgia law, it explained that the loss did not result directly from the computer fraud, but rather only when the card issuer issued funds to pay for the purchases made with the cards. The contrast in these two cases makes clear that an insurance policy's applicable law provision remains one of the most important, yet frequently underappreciated, provisions in any insurance policy (and its ensuing litigation).

For more on this topic in 2019, keep an eye out for the Eleventh Circuit's decision in Principle Solutions v. Ironshore Indemnity Co.[5] This case also involves a fraudster posing as an employee's boss to dupe the employee into wiring money to the fraudster. The crime policy covered "computer and funds transfer fraud" losses resulting directly from a fraudulent instruction directing a financial institution to "debit your 'transfer account' and transfer, pay or deliver" money or securities from that account. The lower court found the policy ambiguous, and therefore found coverage, but also stated that avoiding coverage based on the multiple steps between the fraud and the transfer would render the policy illusory.

Aqua Star (USA) Corp. v. Travelers[6]

A fraudster posed as a vendor in emails, tricking an employee into transferring him money. The computer fraud crime policy covered "direct" hacking, but with an exclusion for "loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." The lower court found no coverage based on the exclusion because the transfer, though fraudulently induced, was technically authorized. The Ninth Circuit affirmed.

Spec's Family Partners Ltd. v. The Hanover Insurance Co.[7]

Rounding out the list, and moving beyond computer fraud insurance coverage for phishing scams, is Spec's Family Partners Ltd. v. The Hanover Insurance Co. Spec's credit card network was hacked. Its contractual partner, First Data, reimbursed banks for the fraudulent transactions resulting from the hack and demanded reimbursement from Spec's. Spec's D&O policy covered any "loss" which the policyholder was legally obligated to pay because of "Claims" made against the policyholder during the policy period, and had an accompanying duty to defend against any such "Claims." "Claims" was defined as any written demand presented for monetary damages or nonmonetary relief for a "Wrongful Act," but excluded loss due to claims against the policyholder arising out of, or attributable to, a contract or agreement, where liability would not have attached in the absence of such contract or agreement. While the lower court found this exclusion barred coverage, the Fifth Circuit disagreed, finding that theories of negligence and general contract law implied possible liability separate from the contractual agreement between First Data and Spec's.

The decision, when combined with other 2018 decisions like Dittman v. UPMC,[8] where the Pennsylvania Supreme Court held that employers owed their employees a duty to exercise reasonable care to protect the employee information stored by the employer, becomes notable as representing a potentially broadening interpretation of traditional concepts. If this trend continues to take hold, 2019 could include increasing liability for companies.

Patricia M. Carreiro is an associate at Axinn Veltrop & Harkrider LLP.

[1] See, e.g., Apache Corp. v. Great Am. Ins. Co. , No. 15-20499, 2016 WL 6090901 (5th Cir. 2016) (finding no coverage); State Bank of Bellingham v. BancInsure, Inc. , 2016 WL 2943161 (8th Cir. 2016) (finding coverage).

[2] No. 17-2492 (2d Cir. 2018)

[3] 895 F.3d 455 (6th Cir. 2018)

[4] 731 Fed. App’x. 929 (11th Cir. 2018)

[5] No., 17-11703 (11th Cir. 2018)

[6] 719 Fed. App’x. 701 (9th Cir. 2018).

[7] 739 Fed. App’x. 233 (5th Cir. 2018)

[8] No. 43 WAP 2017, 2018 WL 6072199 (Pa. Nov. 21, 2018)
