INSURANCE JOURNAL

View this article online: https://www.insurancejournal.com/magazines/ideaexchange/2017/11/06/469990.htm

The Modern Fraudster: How Courts Are Responding to Social Engineering Fraud

Circuit Courts to Clarify Coverage for Social Engineering Fraud

The Second and Sixth Circuit Courts of Appeals are poised in 2018 to clarify a thorny issue for policyholders and insurers alike: the availability of insurance coverage under commercial crime policies for social engineering fraud (SEF).

SEF is an umbrella term for a series of conduct that is simply an extension of the age-old confidence trick. The term refers to a fraudster's ability to manipulate the psychology of the intended victim, playing upon that person's desire to trust, be responsive, and help a superior or client. SEF encompasses the following schemes: impersonation/pretexting, phishing, CEO/fake president fraud, business email compromise, whaling, and spoofing. A common example is a fraudster sending an email requesting payment from an address that closely mimics the email of a business executive or an important vendor. In the age of ubiquitous email, SEF is a major concern for business: 100,000 such attacks occur every day, causing hundreds of millions of dollars in losses annually.

Insurance coverage for victims of SEF may be particularly tricky due to the nature of the attack, as the attack typically relies on voluntary acts by the victims to execute a transfer in funds. This leads to disputes under computer fraud or the funds transfer fraud parts of commercial crime policies since they often require that the loss results directly from the acts of the criminal and/or exclude coverage for voluntary acts. The majority of courts addressing coverage under a commercial crime policy to date for SEF losses have found an absence of coverage for three main reasons.

First, they are reluctant to determine that losses involving email necessarily result directly from the use of a computer.

Second, they are hard-pressed to find that a transfer of funds requested by an authorized person can be a fraudulent transfer.

Third, they find compelling exclusions for "voluntary payments" even when the loss was the product of deception.

The challenges facing policyholders seeking coverage under a commercial crime policy for SEF losses is best seen through American Tooling Center Inc. v. Travelers Casualty & Surety Co. of America, No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017). The coverage dispute arose when American Tooling Center Inc. (ATC) authorized $800,000 in payments to a bank account it believed to belong to one of its vendors. A fraudster using

an email address virtually identical to the vendor's address had instructed ATC to wire the funds to the fraudster's account. ATC sought coverage under its computer crime policy. Its insurer denied the claim, insisting the loss was not a "direct loss" caused by the "use of a computer." ATC then initiated litigation.

Upon cross-motions for summary judgment, the district court ruled in favor of the insurer. The court held the loss was not directly caused by the use of a computer because the real cause was ATC's failure to verify the bank account with the vendor. Thus, due to the intervening events between the receipt of the fraudulent emails and the authorized transfer of funds, it could not be said that the loss was directly caused by a computer. This was in contrast to a funds transfer caused by an infiltration or hacking of ATC's computer systems. Importantly, ATC has appealed this decision to the Sixth Circuit Court of Appeals.

In contrast to ATC, a New York federal court in Medidata Solutions Inc. v. Federal Insurance Co., No. 15-cv-907, 2017 WL 3268529 (S.D.N.Y. July 21, 2017), concluded a fraudulent transfer was a covered loss. Medidata Solutions Inc., a provider of cloud-based services to scientists, used an email platform offered by Google's Gmail. Although the address of Medidata's employees used a domain name specific to the company, emails were still routed through Google's system.

Medidata's finance department had been informed that an acquisition might occur. Its employees were instructed to be prepared to assist with significant transactions. An employee in accounts payable then received an email purportedly from Medidata's president notifying her that an attorney would soon be contacting her regarding an acquisition. The employee later received a phone call from the "attorney" who demanded a wire transfer. She responded that she needed approval from the vice president and the director of revenue. The employee then received an email purportedly from the president approving the payment. Thereafter, she made a payment of nearly $5 million. The "attorney" subsequently made a second demand for payment. That led to the discovery of the fraud.

Medidata sought coverage for the loss under its commercial crime policy, which contained computer fraud and funds transfer fraud parts. The insurer denied coverage, which led to Medidata's commencement of suit. On cross-motions for summary judgment, the district court analyzed the computer fraud coverage and determined a covered fraud was perpetrated. The court found it compelling that the fraudsters "spoofed" the email of the president by embedding computer code. It rejected the argument that the fraudsters had to hack into Medidata's system and execute the transfer themselves in order to trigger coverage.

The court found no requirement of a direct nexus between the sending of the email and the wire transfer. Instead, the court found persuasive that the Medidata employees only initiated the wire transfers based on the instructions in the spoofed emails. Likewise, with respect to the funds transfer fraud coverage, the district court found it sufficient that the transaction was the product of a trick or deception. It was insignificant that the transfer was performed knowingly and by an authorized person. The insurer has appealed this case to the Second Circuit Court of Appeals.

Coverage for SEF claims under commercial crime policies is generally insurer-friendly, but only a handful of jurisdictions have analyzed the issue. Nevertheless, rulings in 2018 from the Second and Sixth Circuits (as well as the Ninth and Eleventh Circuits) should hopefully harmonize the case law and eliminate any schism between the courts.

Alternatively, policyholders may believe they can turn to their cyberinsurance for coverage, but those policies do not apply to SEF. Instead, they respond to the consequences of lost data or network system access, or the hacking of systems to cause the unauthorized transfer of funds. Thus, there is a very real and substantial coverage gap with respect to SEF losses.

Certain commercial crime insurers are now offering specific coverage for SEF, albeit with limits inadequate to respond to many SEF losses. These SEF endorsements or coverages are untested in courts.

Due to the increasing danger of SEF and the uncertain, insufficient coverage currently provided, policyholders should review their policies and consult with their brokers to identify strategies to protect against the economic

consequences of SEF. While insurance protects against economic loss resulting from SEF, it does not stop SEF from happening.

Schwartz is a partner and Willmott is an associate in the global insurance services practice group of Goldberg Segalla. They are based in the Chicago office.

More from Insurance Journal

Today's Insurance Headlines | Most Popular | Idea Exchange, National Section