Turning to Crime Insurance Policies for Phishing Losses

by Dennis Nolan and Joshua Gold

Spear-phishing attacks present significant cyber exposures for businesses in all industries. It is a familiar scenario: A fraudster crafts a communication apparently from a trustworthy source—an executive, a legal advisor, a vendor—and tricks the employee into wiring money to the fraudster's bank account. Once the money hits that account, it disappears with the fraudster. Businesses have lost billions of dollars collectively as a result of these scams.

Certainly, an ounce of prevention is worth a pound of cure. Training employees to recognize suspicious emails and investing in the latest security measures remain the best defense. As spear-phishing attacks become more tailored and technologically more sophisticated, employees increasingly will take the bait and fall victim.

When a loss occurs, employers should promptly consider their insurance coverage, including their crime insurance policies. Crime insurance companies have argued in response to many such claims that their policies only cover brute force, direct "hacks." This past summer, however, two federal appellate courts—the Second Circuit in *Medidata Solutions, Inc. v. Federal Insurance Company*, and the Sixth Circuit in *American Tooling Center, Inc. v. Travelers Casualty & Surety Co.*— contradicted that argument. While not identically worded, the policies in both cases covered losses "directly" resulting from computer fraud, with neither insurance product restricting coverage to brute-force hacking attacks.

In *Medidata*, an employee received an email, purportedly from a Medidata senior executive that included the executive's picture. The cyber fraudster "spoofed" the email code to alter the "From" field to make it look like an email from the executive and requested the transfer of almost $5 million. After emailing and speaking with an "attorney," the employee obtained management approval and wired the money. Federal Insurance Company declined to pay the loss under a policy that included coverage for "direct loss of money" from computer fraud. The policy defined "computer fraud" to include "entry of data into" or changing of data in *Medidata*'s system.

Although *Medidata* conceded that no hack occurred, the Second Circuit found that "the fraudsters nonetheless crafted a computer-based attack that manipulated *Medidata*'s email system." According to the court, the attack introduced the spoofing code into the system, which changed a data element and altered the appearance of the email to fraudulently indicate the sender.

The Second Circuit also found that the employees' intervening actions to transfer the funds pursuant to the fraudulent emails did not make the loss indirect. The court noted that, under New York law, "direct loss" equates to "proximate cause," and here, "it is clear to us that the spoofing attack was the proximate cause of Medidata's losses." The court found that since the employees believed that they were acting at the executive's behest, their actions did not sever the causal relationship between the spoofing attack and the loss.

A week later, the Sixth Circuit, in *American Tooling*, found that an industrial policyholder (ATC) was entitled to crime insur-

RISK MANAGEMENT

Reprinted with permission from Risk Management.
Copyright © 2018 Risk and Insurance Management Society, Inc.
All Rights Reserved.
www.rmmagazine.com

ance for a phishing scam. There, a thief impersonating an ATC vendor intercepted emails requesting the vendor's invoices for payment. Through numerous emails made to look authentic by using an email address very similar to the vendor's, the fraudster instructed ATC's treasurer to wire over $800,000 in payments to various accounts over several months. Travelers refused to pay under its computer crime/fraud policy, arguing that the policy only covered "direct loss" of money "directly caused" by computer fraud.

The Sixth Circuit reversed the district court's acceptance of the insurance company's direct loss defense. It held that under either a proximate cause analysis or a "direct means immediate" approach, ATC's loss was a "direct" one. Applying an analogy to debunk Travelers' arguments, the court explained that if "Alex" owes "Blair" five dollars, and before Alex pays the five dollars, "Casey" snatches the bill from Alex's fingers, "Travelers would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill." Thus, the Sixth Circuit concluded, "ATC received the fraudulent email at step one. ATC employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was the 'point of no return' making the theft from the computer fraud a 'direct loss' to ATC." The court also made clear that "computer fraud" coverage was not limited to "hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer."

With the amount of trickery going into computer-based thefts these days, crime insurance companies too often use the many steps involved in a fraudulent scheme to argue that losses are indirect and otherwise uncovered. The recent decisions of the Second Circuit and Sixth Circuit on the "direct loss" argument and the scope of computer fraud coverage recognize the sophistication and reality of phishing scams, and that the policy language does not distinguish between frauds based on how they induce a transfer. Employers should be familiar with their crime coverage and any policy relating to computer, business email compromise or social engineering fraud and promptly notify all potentially implicated lines of insurance coverage when a cyber incident occurs. ■

Note: The authors were amicus counsel for United Policyholders in the Medidata Solutions, Inc. v. Federal Insurance Company case before the Second Circuit.

Dennis J. Nolan is a shareholder in Anderson Kill's New York office and member of the firm's insurance recovery and cyber insurance recovery groups. **Joshua Gold** is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

Copyright © 2018 Risk and Insurance Management Society, Inc.

All Rights Reserved.

www.rmmagazine.com