ANDERSON KILL
CYBER INSURANCE ALERT

April 2018

Three Appellate Courts to Address the "Direct Loss" Defense Against Insurance Coverage for Spear Phishing Losses

By Daniel J. Healy

Three cases pending in U.S. Courts of Appeal present questions of insurance coverage for spear phishing losses. These cyber losses are often covered by crime policies that have specific provisions providing coverage for computer fraud and fraudulent transfers of money. In the increasingly complex world of computer scams, however, insurance companies are looking to avoid coverage. One often-invoked coverage defense against phishing claims is being put to the test in three pending appellate decisions.

Companies that fall victim to these scams typically have a single employee targeted by a sophisticated email. Recently, insurance companies have relied upon causation arguments to deny coverage, claiming that a tricked employee was not intended to be covered and that only hacks that instruct banks to wire money (without the involvement of the policyholder's employee) are covered.

The cases currently on appeal suggest that policyholders should strongly consider fighting coverage denials for phishing claims, particularly when those denials are based on the meaning of terms like "directly," "indirectly" and "caused by." Each of the cases involved a phishing email sent to an employee of the policyholder. In each case, the employee was deceived by the fraudulent email into believing that the email was a legitimate request for payment, had further contact with the thief who sent it, obtained internal approval to wire money, and arranged a wire to pay the fraudulent request.

Each of the cases also involved relatively similar policy provisions. The coverage grant was not identical in each of the policies at issue, but provided coverage for loss directly resulting from computer fraud. The insurance companies denied coverage — with mixed results — by arguing, in essence, that the coverage only applied to losses from a hacker impersonating the policyholder and directing a bank to wire the policyholder's money to the hacker. Of course, nothing in the policies is actually that specific.

Of the three district court decisions on appeal about this issue, two courts ruled in favor of the policyholder. The Southern District of New York found the policy language provided clear coverage. The Northern District of Georgia held that the language in the policy at issue is

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue
Los Angeles, CA 90071
(213) 943-1444

www.andersonkill.com

who's who

Daniel J. Healy is a partner in Anderson Kill's Washington, D.C. office and is co-chair of the firm's Cyber Insurance Recovery Group. Mr. Healy represents policyholders seeking insurance coverage and has experience obtaining coverage relating to cyber, directors and officers liability, business interruption, environmental liabilities, health benefits, property damage, asbestos products, and intellectual property disputes.

dhealy@andersonkill.com
(202) 416-6547

ambiguous, because if it means what the insurance company claims it means, then coverage would be illusory. The Eastern District of Michigan, on the other hand, narrowly construed the policy language to find coverage only when the loss immediately follows the fraud, with no intervening steps.

Recognizing the Reality of Phishing Scams in Metadata?

The U.S. Court of Appeals for the Second Circuit has received the full briefing for *Medidata Solutions Inc. v. Federal Insurance Co., No.17-2492 ("Medidata").*[1] *Medidata* involves a cyber loss resulting from a phishing scam that fooled Medidata's accounting personnel. The phishing email was directed to an accounts payable employee, purportedly from a Gmail account belonging to Medidata's president. It included a picture of the president and his email address, as well as a copy email address of a fake attorney. The fake attorney "spoofed" the code in the email to make it look like an email from the president, including in the "From" line. The email requested the transfer of $4.8 million. After writing to and speaking with the fake attorney, the employee obtained management approval and transferred $4.8 million to the fake attorney through a bank. Before further money was transferred, the scam was discovered, but the transferred money has not been recovered and the thief's identity is unknown.

Medidata, a technology company, had purchased crime coverage from Federal Insurance Company that included coverage for "direct loss of money, securities or property" from computer fraud or funds transfer fraud committed by a third-party actor. The policy's definition of computer fraud included fraudulent entry of and changing of data in Medidata's system. It further defined the transfer of funds to include transfers performed pursuant to "fraudulent instructions."

Federal nonetheless denied coverage. It claimed the coverage was not for when an employee was tricked into transferring funds, but only for when a hacker breaks into Medidata's computers and transfers funds. In other words, Federal argued that the loss was not caused by the type of loss the policy covered.

The U.S. District Court for the Southern District of New York ruled that Federal was wrong. It held that there was coverage because Medidata's loss happened when a thief changed computer code without permission to make the phishing email appear to be from Medidata's president, when it was not. Additionally, there was coverage under the funds transfer fraud coverage set forth in the Federal policy. The court specifically stated that the mere fact that Medidata's employee "willingly pressed the send button on the bank transfer does not transform the bank wire into a valid transaction."[2]

This ruling is particularly useful for policyholders. By asserting that the actions of an employee victim of a phishing scam negated coverage, the insurance company is essentially attacking the weakest link, much like the scammer who sent the phishing email.

Insurance companies have attacked policyholders who seek coverage by arguing that employees of the policyholder defeated coverage by initiating a transfer of funds. By holding that fraudulent instructions from a scammer are covered as fraudulent whether sent to the policyholder or to a bank, the decision recognizes the sophistication and reality of phishing scams, and that the policy language does not distinguish between them.

Federal has appealed to the Second Circuit and argues that there is no coverage because the policy is intended to cover only those instances where a third party impersonates a Medidata employee to trick a bank into wiring money. The policy language is not limited to such a circumstance. And in today's world Federal's reading would gut the coverage provided in the policy.

Narrowly Construing "Direct Loss": American Tooling

Also on appeal in another case now pending before the U.S. Court of Appeals for the Sixth Circuit, a policyholder faces a coverage denial based on the similar argument that the loss the policyholder suffered was not directly caused by a hacker or by a hacker impersonating an employee of the policyholder company.

In that case, captioned *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America,* No. 17-2014 (6th Cir.), the policyholder's employees were tricked into transferring money by fraud. Much like in *Medidata*, the hackers sent American's treasurer a "spoofed" email purportedly from a Chinese vendor (and made it look authentic using an email address very similar to, but not the same as, the vendor's email address). The email instructed American to pay several legitimate, unpaid invoices to a new, foreign bank account. Without verifying the new bank, American paid $800,000 to the identified account. Numerous emails and payments were sent from March through May 2016.

Travelers denied coverage, contending that the policy covered only "direct loss of, or direct loss from damage to, Money …directly caused by Computer Fraud" and the loss was not caused "directly" by computer fraud. Travelers further argued that "computer fraud" is defined as "the use of any computer to fraudulently cause a transfer of Money" and there were several steps, including authorization by personnel at American, from the date of the first email to the dates of the transfers.

The district court ruled in Travelers' favor,[3] finding no coverage by narrowly reading the coverage to apply only when the loss immediately followed the computer fraud as a matter of causation. That narrow reading of "direct loss" does not square with other cases and raises causation issues intended to defeat otherwise clear coverage.

American has appealed and the case remains pending before the Sixth Circuit. Comparing the rulings in *American* and *Medidata* highlights the complexity of social engineering cases. It underscores why the insurance companies' simplistic view that the risk is only of direct hacks into a computer system is unrealistic.

Tie Goes to the Policyholder: Principle Solutions

Further underscoring the issue, a third case on appeal held that very similar coverage was ambiguous. In *Principle Solutions Group LLC v. Ironshore Indemnity Inc.*, No. 17-11703 (11th Cir.), an employee of Principle (an information technology company) received an email purportedly from the president of Principle asking her to work with an attorney to wire $1.717 million that day. She did; the money was wired after phone calls with the attorney, and of course the email was fraudulent and the imposter attorney was a thief. The president of Principle denies sending the email.

Ironshore denied coverage and argued that the coverage for "Loss resulting directly from" a "fraudulent instruction" to a financial institution to debit the policyholder's account did not apply when the policyholder's employee undertook acts between the fraudulent email and the debit. Again, Ironshore argued the narrow causation argument based on "directly."

The district court disagreed, pointing out that corporate policyholders can only act through the actions of their employees.[4] The court further found the policy language ambiguous. That means it was susceptible to more than one reasonable reading and, because the insurance company wrote it, the tie goes to the runner: there is coverage for the policyholder. Hitting the nail on the head, the district court stated:

> If some employee interaction between the fraud and the loss was sufficient to allow Defendant to be relieved from paying under the provision at issue, the provision would be rendered "almost pointless" and would result in illusory coverage.

Now on appeal, Ironshore argues that the district court failed to read the meaning of "directly" into the policy language to cut off any coverage after the point at which the fraudulent email was sent. The causation argument is very similar to *Medidata* and *Principle*. The issue for the appeals courts deciding these issues is how narrowly to read the term "directly" and whether the term denotes that there is coverage only when the sole and only thing that happened prior to fund transfer was the hacker's fraud. That decision may turn, in part, on whether the policy language requires that the hacker tricked the bank (only) and did not involve the policyholder.

Notably not at issue in these cases are so-called "voluntary parting" exclusions that insurance companies often use to argue that there is no coverage when an employee is deceived. Those provisions should be noted if present in a policy for crime coverage or other first-party coverage that might be relied upon in the event of a cyber loss. Unfortunately, the foregoing cases demonstrate the insurance industry's desire to avoid coverage for cyber losses that involve an employee being tricked into transferring money whether or not "voluntary parting" language is in the policy.

While the appeals courts could reach decisions harmful to policyholders, the underlying case law provides hope that insurance companies will not be permitted to significantly limit the coverage they sold to protect against cyber crimes. Policyholders who have suffered or are trying to prevent losses from phishing scams and other cyber attacks should pay attention to these cases and be prepared to dispute coverage denials.

1 *Anderson Kill, P.C. partners Joshua Gold and Dennis Nolan represent an* amicus curiae *United Policyholders in the Medidata case.*
2 *The cite for the district court ruling is* Medidata Solutions, Inc. v. Fed. Ins. Co., *No. 15-cv-907 (JAC), 2016 U.S. Dist. LEXIS 178501 (S.D.N.Y).*
3 American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America, *No. 16-12108 (E.D. Mich. Aug. 1, 2017)*
4 Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., *No. 15-cv-4130 (RWS), 2016 WL 4618761 (N.D. Ga. 2016).*