JENNER&BLOCK

April 2016

Vol. 3, Issue 4

Insurance Law Update

Can Computer Crime and Fraud Insurance Policies Extend Coverage to Sophisticated Phishing Scams?

By: Mark P. Gaber

PRACTICAL POLICYHOLDER ADVICE

Policyholders should review their Computer Crime and Fraud Insurance Policies and understand whether they could be interpreted to apply only to traditional hacking crimes involving direct access to a computer system, rather than sophisticated new forms of email "phishing" scams involving a fraudulent scheme to induce the transfer of funds. To the extent the policies may limit coverage to direct hacking, policyholders should consider obtaining additional stand-alone cyber liability insurance to cover these emerging phishing attack risks and other cyber crimes where funds are voluntarily transferred by employees through fraudulent inducement.

Three prominent pending cases will test the contours of computer crime and fraud insurance policies to determine whether they cover only traditional hacking of computer systems or whether they extend to sophisticated new forms of email phishing scams. In a traditional hacking scheme, a criminal remotely accesses a computer system without authorization. By contrast, phishing schemes involves human interaction, such as a criminal posing as a company employee by sending official-looking emails. In the pending cases discussed herein, insurers have denied coverage, claiming generally that the computer crime and fraud insurance policies issued are limited to traditional hacking.

In *Medidata Solutions Inc. v. Federal Insurance Co.*, No. 1:15-cv-00907 (S.D.N.Y.), Medidata, a medical technology company, lost $4.8 million in a phishing attack. An accounting department employee at Medidata received an email that appeared to be from a company executive directing the employee to transfer $4.8 million to a Chinese bank account. Copied on the email was a person pretending to be a lawyer who had several conversations—including by phone—with the accounting department employee. The fraud was discovered after the employee transferred the money. Medidata filed a claim with its insurer, Federal Insurance Co. (a unit of Chubb Corp.) under its computer crime and fraud policy.

The policy's "Computer Fraud" coverage protects against loss from "the unlawful taking or fraudulently induced transfer of money . . . resulting from a [c]omputer [v]iolation," which it defines as "the fraudulent entry of [d]ata into . . . a [c]omputer [s]ystem" and "change to [d]ata elements or program logic of a [c]omputer [s]ystem." The policy's "Funds Transfer Fraud Coverage" protects against "direct loss of [m]oney" resulting from "fraudulent electronic . . . instructions" directing a financial institution to pay funds without the knowledge or consent of the organization purportedly issuing the instructions.

Federal Insurance Co. (Federal) denied Medidata's claim, and Medidata sued. Federal, in seeking summary judgment, asserted that the policy extends only to hackers who cause an *involuntary* transfer of money; here, said Federal, the accounting employee voluntarily transferred the money. Moreover, Federal contended that the employee knew and consented to the payment of funds, precluding coverage under the funds transfer provision. Medidata also sought summary judgment, arguing that the modifications to the email to include the executive's name and picture constituted "fraudulent entry of data" and that coverage would be meaningless if it did not apply to fraudulently inducing the voluntary transfer of funds.

On March 9, 2016, the court denied both Medidata's and Federal's motions for summary judgment, ruling that the evidentiary record was insufficient and ordering expert discovery to determine the details by which the phishing attack altered the email and how the email was received. The court's denial of Federal's motion at least suggests that the court may not be convinced by Federal's categorical denial of coverage for phishing attacks eliciting a voluntary transfer of money.

A second, similar case is pending in the Northern District of Georgia, *BitPay, Inc. v. Massachusetts Bay Insurance Co.*, No. 1:15-cv-03238 (N.D. Ga.). BitPay's CFO received an email from an imposter posing as an executive from a prominent bitcoin publication. The email directed the CFO to a website where he entered his login information for his corporate email account. The hacker then sent emails posing as the CFO to obtain bitcoin transfers from one of BitPay's clients. All told, the hacker fraudulently obtained $1.85 million in bitcoins—a form of digital currency.

Massachusetts Bay denied BitPay's insurance claim. The "Computer Fraud" policy provides that the insurer will "pay loss of . . . 'money' . . . resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the 'premises' . . . [t]o a person . . . outside the 'premises'; or [t]o a place outside those 'premises.'" The policy further defines "money" to include bitcoins. Massachusetts Bay contends that the policy only covers fraudulent transfers that come *directly* from the *premises*, *i.e.*, from within BitPay's offices without any intervening steps. Here, says Massachusetts Bay, the hacker caused BitPay's customer to make a fraudulent transfer outside the premises. Massachusetts Bay also draws a distinction between fraudulently *causing* a transfer, which it says the policy covers, and causing a *fraudulent* transfer, which it says happened here and is not covered.

BitPay has countered, among other arguments, that "directly" refers to the type of loss (loss of the bitcoins, as opposed to consequential losses), that the policy only requires the cause of the transfer to be fraudulent, as it was here, and that the policy's express coverage of bitcoins as "money" would be illusory if they were required to be stored on "premises"—as the very nature of bitcoins is virtual.

Massachusetts Bay sought to bifurcate discovery to avoid discovery related to BitPay's bad faith claim. On March 17, 2016, the district court denied that request and ordered Massachusetts Bay to produce all responsive documents.

Finally, in another case against Federal Insurance Co., *Ameriforge Group, Inc. v. Federal Insurance Co., et al.*, No. 16-cv-377 (S.D. Tex.) an email phishing scheme has also been denied coverage. In that case, a fraudster imposing as Ameriforge's CEO sent an email to the company's accounting department instructing the transfer of $480,000 to a Chinese bank, instructing that the task was a top priority and confidential, that a KPMG lawyer would be in contact with the employee, and that communication about the task should only occur in response to the email. After the fake lawyer called the employee, the funds were transferred.

Federal denied coverage, asserting (i) that the policy's forgery coverage was limited to forgeries of actual financial instruments and not fraudulently signed emails directing the transfer of funds; (ii) that the policy's computer fraud coverage requires a hacking event whereby unauthorized access to the computer system occurs, not merely a phishing attack through an email; and (iii) that the funds transfer fraud coverage does not cover situations in which funds are knowingly transferred, even if fraudulently induced. For purposes of these coverages, "Computer Fraud" is defined as "the unlawful taking of Money, Securities or Property resulting from a Computer Violation." "Computer Violation" is in turn defined as an unauthorized "entry into or deletion of Data from a Computer System," "change to Data elements or program logic of a Computer System, which is kept in machine readable format," or "introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System." A "Computer System" is defined to include "communication facilities," and "Data" means information contained in records, manuscripts, accounts, microfilms, tapes or other records, which are processed and stored in a Computer System."

It is too early to tell whether insurers asking courts to strictly interpret computer crime and fraud insurance policies to apply only to traditional hacking will prevail, or whether these types of policies will be broadly interpreted to also cover sophisticated new forms of phishing attacks, where company employees are fraudulently induced into transferring funds. As with most insurance cases, the result will likely turn on the specific facts and the individual policy provisions. Accordingly, these cases highlight the importance of carefully reviewing policy terms to ensure that phishing attacks—a growing source of cyber crime and fraud—are covered.

Mark P. Gaber would like to thank Jan A. Larson (partner, Washington, DC) for her contributions to this article.

Contact Us

Mark P. Gaber
Associate

Phone: 202 637-6367
Email: mgaber@jenner.com
Download V-Card

Jan A. Larson
Partner

Phone: 202 639-6046
Email: janlarson@jenner.com
Download V-Card