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

# Phishing For Coverage Under Crime Policies

By **Marc Schein and Robert Chesler**

*Law360, New York (May 22, 2017, 11:32 AM EDT)* -- Crime policies, among others, typically provide what seems like a broad grant of computer coverage, such as "We will pay for loss … resulting directly from the use of any computer to fraudulently cause a transfer … ." Apache Corp. v. Great American Insurance Co., 2016 WL 6090901(5th Cir. 2016). Companies victimized by phishing schemes have sought coverage under the computer provisions of their insurance policies for their losses. They have met with no success in the courts.

Marc Schein

Robert Chesler

The preliminary question is: what is phishing? In brief, it's a fraudulent attempt usually delivered by email, to induce a target to reveal sensitive information, such as passwords or credit card numbers — or to wire money directly as instructed by the fraudster. Typically, a phisher will send out thousands, sometimes millions, of emails that appear to come from a known party or a trusted company. The attack tries to evoke an emotional response to a hoax crisis. It's not uncommon for the email to direct the recipient to send money to a spoofed website. Phishing schemes have become very common, and can result in substantial losses. Unless a company has the right policies and procedures in place to detect phishing attacks, it is possible the attacks can continue for months, even years. Practices to prevent phishing losses should include: 1) make sure employees know how to identify suspicious emails; 2) never go to a bank's website from a link found in an email; 3) audit your company's network security; 4) review the email address of the sender of the email for inconsistencies and variations in spelling; 5) check your financial accounts frequently; 6) input sensitive data through secure web portals only; and 7) implement two factor authentication.

Apache is a typical phishing case. It involved "authorized payments of legitimate invoices from its vendor to the criminal's bank account … ." Apache received an email attachment on its vendor's letterhead with old and new (fake) bank account numbers. Apache called the number on the letterhead to confirm the change in bank account numbers. Apache then approved the change and wired money to the fake bank account. Apache had not noticed that while the vendor's email address was "petrofac.com," the sender's address on the email was "petrofactltd.com," a fraudulent email created by the criminals. Within one month, the real Petrofac asked where its money was, and Apache uncovered the scheme and found it had lost about $2,400,000. Apache made a claim for the loss under the computer provision of its crime policy with Great American Insurance Company. Great American denied coverage, and coverage litigation ensued.

The trial court found the insurance policy covered Apache for the loss. It rejected Great American's argument that the loss was not direct because of intervening factors — "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor.'" The Fifth Circuit reversed, finding that the only "computer use" was the use of the email as part of the overall scheme. The court then found that "the email was merely incidental to the occurrence of the authorized transfer of money … To interpret the computer fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would … convert the computer fraud provision to one for general fraud."

Taylor & Lieberman v. Federal Insurance Co., 2017 U.S. Lexis 42056 (9th Cir. 2017), another phishing case, is also instructive. Taylor & Lieberman, an accounting firm, suffered a phishing loss resulting from emails instructing it to wire money to fake accounts. Taylor & Lieberman sought insurance coverage under its fidelity policy, which provided coverage for forgery, computer fraud and funds transfer fraud. The Ninth Circuit found that none of these coverage grants provided coverage for the loss. In particular, the policyholder argued that the computer fraud coverage should apply, inter alia, to unauthorized entry into the computer system. The court held that the sending of an email was not an unauthorized entry.

Incomm Holdings Inc. v. Great American Insurance Company, 2017 WL 1021749 (N.D. Ga. 2017) involved prepaid debit card system fraud. The court held that the policyholder's loss was not direct. Great American Insurance Company argued that the fraud was committed using a phone rather than a computer. The crime policy read as follows: "The Insurer will pay for loss of, and loss from damage to, money, securities, and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises." Once again, the court found that the loss was not directly caused by a computer.

Conversely, at least one court found coverage for hacking — that is, an invasion of a company computer system that involved an employee's error, but not her direct action to transfer funds. In Bank of Bellingham v. BancInsure Inc., 823 F. 3d 456 (8th Cir. 2016), a secretary accidentally left her computer on all night, and a hacker accessed the system. The bank had a financial institution bond that included insurance coverage for computer system fraud. The insurance company argued against coverage, asserting that the secretary was the efficient proximate cause of loss. The court disagreed, and held that the hacking was the efficient proximate cause.

What distinguished Bank of Bellingham from the phishing cases? Insurance companies have different attitudes toward hacking and phishing. In hacking, the computer is central; emails need not be involved. With phishing, the use of a computer may be limited to emails. A hacker's entry into the computer is fully unauthorized, whereas with phishing, the entry is permitted by the company through the phisher's subterfuge. Moreover, hacking does not involve any voluntary action by the company. With phishing, insurance companies contend that the transfer of funds is voluntary, even if fraudulently induced. Finally, all of these issues contribute to the insurance companies' argument that phishing losses are not 'directly' related to the computer.

Help may be on the way. Some insurance companies have now taken notice of policyholders' need for phishing coverage, and are addressing this issue — for example, by including phishing coverage in their crime policy when requested by a broker to an insurance company. Cyberinsurance policies are able to cover loss from phishing if the policy provides a cybercrime element. To avoid coverage gaps, the crime policy should work in coordination with the cyberinsurance policy to provide a holistic approach to the phishing exposure and also other cyber exposures. This is a clear example where policyholders need to think of their insurance brokers as strategic partners, rather than vendors who provide quotes. It is imperative to conduct due diligence to find the right broker who has the knowledge and market knowledge to obtain the best available coverage and policy wording. Moreover, the insurance professional with whom a company works should understand its business and risk tolerance.

---

*Marc D. Schein, a certified insurance counselor and commercial lines coverage specialist, is a risk management consultant for Marsh & McLennan Agency LLC.*

*Robert D. Chesler is a shareholder at Anderson Kill PC's office in Newark, New Jersey. He is a member of the firm's cyberinsurance recovery group.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

---