LOS ANGELES
Daily Journal
www.dailyjournal.com

THURSDAY, DECEMBER 8, 2016

INSURANCE LAW UPDATE

Court limits phishing attack coverage

PRACTICAL POLICYHOLDER ADVICE

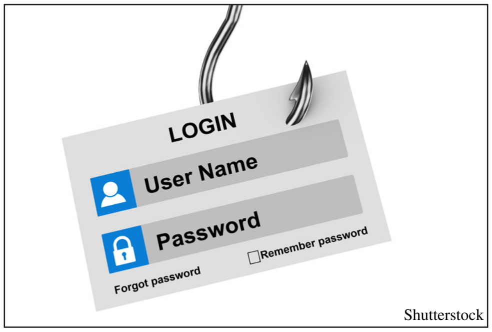
Unlike traditional computer-hacking attacks, which generally involve criminals who gain unauthorized remote access to a computer system, sophisticated phishing schemes rely on human interaction; such schemes commonly involve a criminal who holds herself out as the agent of a legitimate business in order to gain access to another entity's funds or data. In response to policyholders' attempts to seek coverage for these types of phishing attacks under traditional computer crime and fraud policies, a growing number of courts have narrowly interpreted these policies' causation language to require that the loss result directly from a computer fraud, without any intervening acts such as an employee acting at the direction of a cybercriminal. As a result, policyholders should carefully review and understand the terms of any existing computer-fraud coverage and consider obtaining policy endorsements specifically designed to cover sophisticated phishing attacks, or a stand-alone cyber liability policy.

By Karthik P. Reddy and Jan A. Larson

Recently, in *Apache Corp. v. Great American Insurance Co.*, 15-20499 (5th Cir. Oct. 18, 2016) (per curiam), the 5th U.S. Circuit Court of Appeals weighed in on the ongoing debate surrounding the scope of computer-fraud coverage when it considered whether a computer-fraud provision in a crime-protection policy underwritten by Great American Insurance Company required Great American to indemnify an insured's losses resulting from a multimillion-dollar phishing scheme. After canvassing available opinions from state and federal courts, the 5th Circuit cast its lot with a number of courts that have limited computer-fraud coverage to losses attributable to direct hacking.

While the *Apache Corp.* case is distinguishable on its facts and also involved an alleged lack of due diligence by the policyholder, the decision nevertheless may be viewed as a reason for policyholders to reexamine their traditional insurance policies and consider whether stand-alone cyber liability insurance is necessary to fill any potential gaps in coverage. Such caution may be warranted unless and until courts afford greater weight to the fraudulent aspects of phishing schemes arguably worthy of coverage under crime-fraud policies designed to address losses attributable to these and other types of fraud perpetrated on policyholders.

The security breach that culminated in the *Apache Corp.* coverage dispute began when a cybercriminal posing as an agent of Petrofac Facilities Management Limited contacted an employee of the Scottish subsidiary of Apache Corporation, a large Texas-based oil-and-gas company. Notably, the initial contact took place over the telephone, rather than through a computer attack or other hacking incident. The caller, who apparently knew that Petrofac was a vendor that regularly performed work for Apache, informed the employee that Petrofac had recently changed its bank account information and requested that Apache update the routing information that it used to wire Petrofac money for its services. In accordance with internal procedures, the employee who took the call informed the caller that Apache could not process such a request over the phone and instructed the caller to submit a written request on Petrofac letterhead instead.



Shutterstock

The 5th Circuit's reasoning ... may be particularly persuasive as other courts begin to confront insurance disputes involving sophisticated phishing-related liability with increasing frequency.

Five days later, Apache's accounts- payable department received an email from a "petrofacltd. com" address, which bore more than a passing resemblance to Petrofac's authentic email domain, "petrofac.com." Just as the caller did over the phone, the email's author represented herself as an agent of Petrofac, informed Apache of the purported change in Petrofac's bank account information, and requested that Apache begin wiring invoice payments to the "new" account number. In an apparent effort to comply with Apache's official-notice requirement, the sender also attached a signed letter printed on forged Petrofac letterhead repeating the instructions to "use the new [bank] account with immediate effect." As the 5th Circuit would later emphasize, this "computer-use" on the part of the cybercriminal was a response to Apache's own refusal to "transcribe the change-request," which Apache "could have [instead] investigated with its records."

Instead of checking Apache's own records for Petrofac's contact information, an employee in Apache's accounts- payable department read the email and called the number listed on the forged Petrofac letterhead in an attempt to verify the routing information that Apache had received. After someone purporting to be a Petrofac employee answered the call and confirmed the information, Apache's employee submitted an internal request for approval to change Petrofac's account numbers in Apache's payment system. Once an accounting manager approved the request, Apache began making invoice payments to the fraudulent bank account. Apache made a total of $2.4 million in payments to the cybercriminals before receiving a letter from Petrofac inquiring about the firm's delinquent bills. Apache eventually launched an investigation and discovered that it had been the victim of a sophisticated phishing attack.

Apache subsequently submitted a claim to Great American under a crime-protection policy underwritten by the insurer and issued for the relevant time period. That policy's computer-fraud provision obligated Great American to indemnify Apache "for loss[es] ... resulting directly from the use of any computer to fraudulently cause a transfer of ... property from inside the premises ... to a ... place outside those premises." After receiving Apache's claim, Great American denied coverage, explaining its view that the policyholder's "loss did not result *directly from* the use of a computer" because of the human intervention that took place between the fraudulent email and the loss to Apache. (Emphasis added). Apache responded to the coverage denial by filing suit in Texas state court against Great American, alleging that the insurer's denial of coverage was contrary to the terms of the computer-fraud policy. After Great American removed the action to federal district court in the Southern District of Texas, both parties moved for summary judgment.

The district court ruled in favor of Apache. Following *First National Bank of Louisville v. Lustig*, 961 F.2d 1162 (5th Cir. 1992) — a case involving the practical import of the words "resulting directly from ... fraud[]" in a banker's blanket bond — the district court interpreted the policy's reference to losses "resulting directly from" computer fraud as referring to any loss in which computer fraud was a "substantial factor." For this reason, even though several "intervening steps" in the phishing attack against Apache separated the cybercriminals' use of a computer and the transfer of payments to the criminals' fraudulent account, the central role that the fraudulent email played in the scheme convinced the court that Great American had an obligation to indemnify Apache. Importantly, after giving due weight to the policyholder's reasonable expectations of coverage that a "crime protection" policy would, in fact, cover losses caused by what everyone — including the insurer — deemed to be a crime, the court concluded that a more limited reading of the computer- fraud provision would risk "limit[ing] the scope of the policy to the point of almost non-existence," with only direct hacking attacks covered.

Great American appealed the district court's ruling and the 5th Circuit reversed. In a unanimous per curiam opinion, the 5th Circuit held that the computer-fraud provision did not cover the loss that Apache suffered. Given the Texas Supreme Court's "preference for 'uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions,'" the 5th Circuit began by canvassing the few available decisions from state and federal courts and concluded that there is generally "cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events" and did not follow directly from the computer fraud. The 5th Circuit's survey did not, however, reveal exactly what would constitute an event that follows immediately from a computer fraud. Nor did Apache's policy contain any provision addressing this causation requirement in a manner sufficient to place the policyholder on notice of what factors or conditions might be necessary to trigger coverage. In the absence of any guidance, the 5th Circuit observed that, although a fraudulent email was certainly "part of the [cybercriminals'] scheme," it was merely an intermediate step in a "multi-step ... process that ended in" Apache's employees making payments to a fraudulent account. From this, the 5th Circuit concluded that the transfer did not result "directly from" computer fraud, and that Great American had no obligation to indemnify the loss.

The 5th Circuit's decision in *Apache Corp.* represents a narrow view of causation that, for now, may well have consequences for other policyholders of computer-fraud coverage. Given the relative dearth of applicable appellate precedents, the 5th Circuit's reasoning in *Apache Corp.* may become relevant as other courts begin to confront insurance disputes involving phishing- related liability with increasing frequency.

Nevertheless, it remains to be seen what weight other appellate courts give to *Apache Corp.* One thing that distinguishes the 5th Circuit's ruling is that the court emphasized that Apache's employees' unknowing participation in the fraudulent scheme diminished the legal import of the cybercriminals' "computer use." The 5th Circuit was highly critical of Apache's internal procedures and what the court saw as the firm's lack of diligence in properly verifying the cybercriminals' change-of-information request. Such failures on the part of the policyholder may not be present in every successful phishing attack. Additionally, in sharp contrast to the district court's concern over excessively limiting coverage, the 5th Circuit expressed concern that, in an era in which "few — if any — fraudulent schemes [do] not involve some form of computer-facilitated communication," a broader view of causation could "convert [every] computer-fraud provision [in]to one for general fraud." While this apprehension may have steered the court toward a more restrictive interpretation of Apache's policy language, it is up to the insurer to limit the coverage afforded through the use of express and unambiguous terms and exclusions.

With sophisticated phishing schemes being reported with increasing frequency, we expect that more appellate courts will have the opportunity to weigh in on the scope of computer-fraud policies and the application of the particular causation language therein. In the meantime, investments in data security and personnel training can help corporate policyholders minimize the risk of attacks like those suffered by Apache. In addition, unless and until courts have an opportunity to examine what insurers' underwriters intended when issuing computer-fraud policies, policyholders may do well to re-examine the precise language of their computer- fraud policies and consider whether an endorsement specifically designed for phishing attacks, or a stand-alone cyber liability policy, may be appropriate.

Karthik P. Reddy *is an associate in Jenner & Block's Litigation Department. He may be contacted at kreddy@jenner.com.*

Jan A. Larson *is a partner in Jenner & Block's Insurance Recovery & Counseling Practice. She represents policyholders nationwide in complex litigation with their insurers involving a variety of insurance claims. She may be contacted at janlarson@jenner.com.*

KARTHIK REDDY

JAN LARSON