CARLTON FIELDS

Insurers Must Be Prepared For Cybercrime Coverage Battles

June 07, 2016

Financial institution bonds come in various forms, depending on the nature of the insured business (e.g., bank, broker, insurance company). Common forms are fidelity bonds and commercial crime policies. These policies provide first party coverage against losses caused by employee dishonesty, forgery, kidnap, ransom and extortion, computer fraud and other specified financial frauds. These policies are common, and in some cases required by law, for banks, insurers and any entity that has access to or holds funds for others.

These policies are also proving to be fertile ground for coverage battles regarding emerging cybersecurity threats, both within and outside organizations. As we have reported, a New York Appellate Division panel held that such a policy did not cover a Medicare fraud scheme perpetrated by employees under such a policy's "computer fraud" coverage, because the use of a computer to make false entries about medical treatments that were never provided was merely incidental to the fraud scheme. The loss was not caused by "the entry or change of electronic data." Rather, the court held, this type of coverage was intended to cover "hacking" type incidents, not the authorized use of a computer system by a health care provider to effectuate a Medicare fraud scheme.

Meanwhile, a New York federal court is struggling with whether a phishing scam perpetrated against a medical data services provider could be covered under a similar policy. An employee of Medidata Solutions Inc. wired funds based on instructions in a fraudulent email that purported to be from the employee's supervisor, causing an unrecoverable loss of some $4.8 million. Medidata's insurer declined coverage and Medidata sued in New York's Southern District Court. That court recently denied both the policyholder's and insurer's cross-motions for summary judgment, on the basis that it needed additional information. It ordered:

> Both motions for summary judgment are denied without prejudice due to an insufficient record. Parties are granted leave to conduct limited expert discovery. This discovery should be limited to establishing the method in which the perpetrator sent its emails to the plaintiff and discussing what changes, if any, were made to the plaintiff's computer systems when the emails were received. See Medidata Solutions Inc. v. Federal Insurance Co., No. 1:15-cv-00907 (S.D.N.Y. Mar.

10, 2016).
The same issue is now also teed up before the U.S. Court of Appeals for the Fifth Circuit. There, an insurer appealed a decision whereby a Texas federal court found coverage for a similar phishing scam — where an employee was duped by an email into altering wire transfer instructions that resulted in a fraudulent transfer of funds. See Apache Corp. v. Great American Insurance Co., No. 4:14-CV-237 (S.D. Tex. Aug. 7, 2015). The appeal has been briefed and will likely be argued soon.

Now, the Eighth Circuit Court of Appeals has weighed in a case that involves a somewhat more sophisticated hacking scheme that allowed funds to be fraudulently transferred by wire from a bank in Minnesota to a bank in Poland, most of which was unrecoverable, resulting in a $485,000 loss.

In State Bank of Bellingham v. BancInsure Inc., No. 14-3432 (8th Cir. May 20, 2016), the Eighth Circuit affirmed a district court decision in favor of the plaintiff bank in a coverage dispute with its insurer over whether the loss was covered under its financial institution bond.

The court recited the following factual record about the manner in which the fraud was perpetrated: wire transfers were made through a desktop computer at the bank connected to a Virtual Private Network device provided by the Federal Reserve, called FedLine. In order to complete a wire transfer via FedLine, two bank employees had to enter their individual usernames, insert individual physical tokens into the computer and type in individual passwords and passphrases.

A bank employee completed a FedLine transaction using her token, password and passphrase as well as the token, password and passphrase of a second employee. At the end of the work day, she left the two tokens in the computer and left the computer running. When she arrived at work the next day, she discovered that two unauthorized wire transfers had been made to two different banks in Poland. One of the transfers was ultimately unrecoverable, resulting in the loss.

After an investigation, it was determined that a "Zeus Trojan horse" virus had infected the employee's computer, permitting access to the computer for the fraudulent transfers.

The bank sought coverage under its financial institution bond, and the insurer declined, based on certain exclusions in the policy, which it claimed governed whether the excluded causes were direct or indirect.

The policy covered, in relevant part:

> H. Loss resulting directly from a fraudulent
>
> (1) entry of electronic data or computer program into, or
> (2) change of electronic data or computer program within any

> computer system operated by the insured ... provided the entry or change causes
>
> (1) property to be transferred, paid or delivered,
> (2) an account of the insured or of its customer to be added, deleted, debited or credited, or
> (3) an unauthorized account or fictitious account to be debited or credited.
>
> In this Insuring Agreement (H), fraudulent entry or change shall include such entry or change made by an employee of the insured acting in good faith (1) on an instruction from a software contractor who has a written agreement with the insured to design, implement or service programs for a computer system covered by this Insuring Agreement (H) or (2) on an instruction transmitted by tested telex or similar means of tested communication identified in the application for this bond purportedly sent by a customer, financial institution or automated clearing house.

The policy contained a number of exclusions that BancInsure relied on in declining coverage as well, including "(4) loss resulting directly or indirectly from theft of confidential information ... [or] (12) loss resulting directly or indirectly from (a) mechanical failure, faulty construction, error in design, latent defect, fire, wear or tear, gradual deterioration, electrical disturbance or electrical surge which affects a computer system, (b) failure or breakdown of electronic data processing media or (c) error or omission in programming or processing."

The district court granted summary judgment to the bank on the coverage issue, utilizing an efficient proximate cause analysis to determine that "the computer systems fraud was the efficient and proximate cause of [the] loss," regardless if other noncovered causes contributed. It awarded the bank $620,000, which included prejudgment interest.

On appeal, BancInsure challenged the application of concurrent-causation doctrine, which it argued does not apply to financial institution bonds, and, even if it did apply, the parties contracted around the doctrine in the language of the applicable exclusions. BancInsure also challenged the determination that the fraudulent conduct of hacking into the computer system was the efficient and proximate cause of the loss, rather than employee negligence, or other excluded causes.

The Eighth Circuit affirmed. First, it noted that financial institution bonds have consistently been treated as insurance under Minnesota law, and policyholders are entitled to all the common law presumptions in favor of insureds in coverage disputes. The court cited Minnesota's general rule on concurrent causation: "[a]n insured is entitled to recover from an insurer when cause of the loss is not excluded under the policy. This is true even though an excluded cause may also have contributed to the loss."

The court rejected BancInsure's argument that this imposes a higher standard-of-proof on the

insurer to establish that a loss was caused by an excluded cause, and essentially would write the exclusions out of the policy in many situations. It noted that the bank still had the burden to demonstrate coverage in the first instance by showing that its loss was directly caused by the covered peril, in this case the fraudulent wire transfer.

The court also rejected the insurer's argument that the language used in certain exclusions included the term "indirectly" and thus the contract itself rebutted application of the concurrent causation doctrine. The court noted that, while it is true that Minnesota law recognizes parties' ability to knowingly "contract around" concurrent causation doctrine, to do so, the language must be specific. It cited a recent example, Ken Johnson Properties LLC v. Harleysville Worcester Summary Insurance Co., No. 12-1582, (D. Minn. Sept. 30, 2013) (recognizing language that an exclusion applies "regardless of any other cause or event that contributes concurrently or in any sequence to the loss" constitutes an adequate "anti-concurrent causation" provision and "evidences the parties' intent to contract around the concurrent causation doctrine.")

Here, the court held, simply using the term "indirectly" in some exclusions is not a sufficient invocation of the "anti-concurrent causation" provision and thus the doctrine applied. The court held that the malware attack and fraudulent transfer was the efficient proximate cause of the loss, despite possible concurrent causes that may or may not have been excluded.

It will be interesting to see what the Fifth Circuit Court of Appeals will do in the Apache case, and what the Southern District of New York will do in the Medidata case. Those cases are most similar to each other, but both are dissimilar in important ways to both Universal American Corp., where the New York Appellate Division found no coverage for a Medicare fraud scheme effected by employees through the use of a computer system, and Bellingham Bank, where the Eighth Circuit found coverage for a transfer effected through a malware attack by unknown users directly manipulating the insured's computer system. In both Medidata and Apache, it is clear that the losses were caused at least in part by a fraudulent scheme that was initially carried out through transmission of an email by an anonymous bad actor. But these were phishing scams, which may or may not be considered to the type of classic "hacking" event for which the New York Appellate Division found such coverage to be intended, and which was at issue in Bellingham Bank, and they may not have involved any direct manipulation of the insured's computer systems. Clearly, the court's ruling on summary judgment in the Medidata case indicates it will be looking closely at that issue. Insurers and financial institutions and others that hold these bonds should look closely at the issue as well, as an ounce of prevention can be worth a gigabyte of cure. *Republished with permission by Law360 (subscription may be required). Originally published by PropertyCasualtyFocus.*

Authored By

John C. Pitblado

Related Practices

Cybersecurity and Privacy

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.