New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878
An ALM Publication
VOL. 222 NO. 34 MONDAY, AUGUST 29, 2016 NJLJ.COM

INSURANCE LAW

New World of Cyber Insurance Is Starting to Mature

By Robert Chesler

Currently, about 60 different insurance companies participate in the cyber insurance marketplace. No standard forms exist—it is like the Wild West. Cyber policies typically are tightly written, often with over 50 definitions and 50 exclusions, and are designed to cover specifically defined risks. While thus far there have been relatively few coverage disputes, the combination of lack of uniformity and tight drafting creates many coverage pitfalls. The experience of the restaurant chain P.F. Chang's, in its pursuit of cyber coverage after a data breach, illustrates how a seemingly straightforward claim can run afoul of one of dozens of exclusions the policy is likely to contain.

P.F. Chang's

In *P.F. Chang's v. Federal Insurance Co.*, 2016 U.S.Dist. LEXIS 70749 (D. Ar. May 31, 2016), the court commenced its decision by citing the wide breadth of the federal cyber-policy as marketed by Federal on its website: A flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world that "*covers* direct loss, legal liability, and consequential loss resulting from *cyber* security breaches."

Unfortunately for the insured, despite Federal's promise of broad coverage, Federal denied P.F. Chang's cyber claim, and the court upheld the denial.

P.F. Chang's claim was neither exotic nor esoteric. As explained by the court, P.F. Chang and other merchants are not allowed to process credit card transactions. The merchants use servicers who handle the transactions with the companies issuing the cards. P.F. Chang used Bank of America Merchant Services (BAMS), which in turn utilized MasterCard.

On June 10, 2014, P.F. Chang learned that it had suffered a data

Robert Chesler (rchesler@andersonkill.com) is a shareholder in the Insurance Recovery Group at Anderson Kill, practicing in the firm's Newark office.

breach by computer hackers involving about 60,000 credit cards. MasterCard charged BAMS with three assessments totaling almost $2 million. Before discussing the court's decision, it should be noted that, as the court emphasized, Federal did reimburse P.F. Chang for about $1.7 million in damages, including forensic investigation costs and defense of litigation brought by customers and by a bank.

Federal's seemingly schizophrenic denial of the BAMS claim is reflective of the pitfalls often latent in cyber insurance policies, which cover tightly defined risks. In the fast-moving cyber world, risks appear and mutate with breakneck speed, so that a cyber policy can quickly become out of date.

P.F. Chang first asserted that Federal should provide coverage because P.F. Chang had received a claim alleging a privacy injury. However, the court reasoned that the claim against P.F. Chang came from BAMS, which had not suffered a privacy injury. The court was not impressed by the fact that the BAMS claim was merely a pass-through for the claim by MasterCard, which had incurred a privacy injury. This certainly seems a debatable conclusion.

Indeed, the court found for P.F. Chang on the next, similar issue. P.F. Chang asserted that there was coverage for privacy notification expenses incurred by an insured. Federal argued that P.F. Chang did not incur any such expenses. However, the court found that Arizona courts construed "incur" broadly, and although the reimbursement fee was originally payable by BAMS, P.F. Chang had incurred it.

However, what the court gives, it can also take away—the court found that two exclusions barred coverage. One exclusion was for contractual liability, and a second for liabilities assumed by the insured. The court found that since all of P.F. Chang's exposure flowed through its contract with BAMS and assumption of liabilities, no coverage existed.

Currently, about 60 different insurance companies participate in the cyber insurance marketplace. No standard forms exist—it is like the Wild West.

The *P.F. Chang* decision demonstrates that a cyber insurance policy is not a panacea. A claim by BAMS against P.F. Chang was foreseeable. The structure was designed so that BAMS' liabilities were passed through to P.F. Chang. P.F. Chang probably never thought that a court would apply the contract exclusion on these facts.

Some insurance practitioners predict that P.F. Chang will inaugurate a wave of cyber-insurance litigation, but this may be overstated. The fact is, P.F. Chang is the first substantive decision on a cyber-insurance policy in the decade that the insurance industry has offered this product. Anecdotally, the insurance industry has been paying on cyber claims. P.F. Chang may just represent a narrow issue that more careful drafting can eliminate.

Cyber Endorsements

Many companies that do not purchase cyber policies do have cyber endorsements on crime, executive liability or other types of policies. Insurance companies have been more litigious with respect to such endorsements. One area where the insurance companies have drawn a bright line is between hacking and phishing. With hacking, someone breaks into a computer system and steals data or causes damage. With phishing, an outsider convinces an authorized user inside the company that the outsider is an authorized user or client of the company, and typically arranges a wire transfer to a fake address.

Under cyber endorsements, insurance companies have reportedly honored hacking claims but denied phishing claims. In *Universal American Corp. v. National Union Fire Insurance Co.,* 37 N.E. 3d 78 (N.Y. June 25, 2015), the insurance policy provided coverage for "fraudulent entry." The court found that fraudulent entry into a computer system was limited to outside hackers, not fraudulent content submitted by authorized users.

This issue is currently before the Southern District of New York

in *Medidata Solutions v. Federal Insurance Co*. Medidata was tricked into wiring $4.8 million into a false account. Medidata's Federal Executive Protection Portfolio Policy included coverage for computer fraud, funds transfer fraud and forgery. Federal denied coverage, stating that its policy covered "involuntary transfers effected by hackers, forgers and imposters, not voluntary transfers effected by authorized signatories." The court denied both parties' summary judgment motions, and the case is now in discovery.

A second issue that has resulted in claims is whether a loss is "directly" caused by the use of the computer pursuant to the policy. In *Apache Corp. v. Great American Insurance Co*., No. 4:14-cv-237 (S.D. Texas 2015), a crime policy included computer coverage if loss resulted directly from the use of any computer. In this phishing case, a secretary received a fraudulent email, showed it to another employee, who then passed it to a supervisor. The insurance company argued that the loss was not directly caused by the computer, but rather by the intervention of the three individuals. The court disagreed and found coverage.

Bank of Bellingham v. BancInsure, No. 14-3432 (8th Cir., 2016), is similar. In this case, the bank had a financial institution bond that contained computer systems fraud coverage. A secretary forgot to turn off the computer overnight, and hackers accessed the computer. The insurance company asserted that there was no coverage, arguing that the secretary was the efficient cause of the loss. The court found that the hacking was the efficient proximate cause, and held for coverage.

Cyber Insurance Policies

Given the complexity of cyber policies and lack of uniformity in the market, it is critical to have an experienced insurance professional guide a company through this morass and procure the coverage that matches the company's needs. Unfortunately, this is not easy, because expertise on cyber insurance is still sparse in the broker and consultant community.

Some insurance companies sell composite policies, which include multiple coverage modules. The policyholder can select those modules that it believes it needs. These policies typically include first-party coverage for damage to the policyholder itself, and third-party coverage that applies to claims against the policyholder. The third-party coverages may include network and privacy liability; crisis management; regulatory liability; notification costs/identity monitoring; and transmission of viruses/malicious code. First-party coverages include business income loss/extra expense; system failure; information asset and data restoration/recovery; extortion; and forensic investigation. In the past, many companies did not purchase extortion coverage. However, in view of the growth of ransomware cases, this is likely to change.

As cyber professionals like to say, the devil is in the details when reviewing cyber policies. As an example, many policies will have sub-limits for certain coverages. Thus, a company might think that it has $1 million, when there is a $200,000 sublimit for notification costs. As another example, all cyber policies have some form of "war and terrorism" exclusion, but these exclusions can differ dramatically. The war and terrorism exclusion may apply to cyber terrorism, which is defined differently in different policies. A policy may or may not include an exclusion for "acts of foreign enemies," for example—a crucial issue in this age of hacking by North Korea and Iran, for example. Are those countries foreign enemies?

Conclusion

From a lawyer's standpoint, cyber insurance is complex and murky. Indeed, many lawyers need to ask if they themselves should purchase this type of coverage. In a year from now, we should know if *P.F. Chang* is a solitary outlier, or the beginning of a tidal wave. In the meantime, every company should examine whether it needs cyber insurance, and if so, what policy best fits its needs.■