BARNES & THORNBURG LLP

Who Gets Coverage?

December 19, 2017 | | Cyber Insurance, Data Breach, Data Security, Indiana Insurance Coverage, Insurance, Policyholder Protection

Scott N. Godes
Partner
Data Security and Privacy Co-Chair

When a retailer or merchant purchases a broad cyber insurance policy to cover hacks or breaches of its point of sale systems, it could be forgiven for thinking that its insurance policy would cover the costs of fraudulent charges and card replacement costs – which can represent the majority of damages generally incurred in a payment card incident – demanded by the payment processor or the card brands. But one recent decision in the Federal District Court of Arizona has held that certain cyber insurance policies do not provide coverage for those damages. *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*, 2016 WL 3055111 (D. Ariz. May 31, 2016), *appeal dismissed pursuant to settlement*, No. 16-16141, Dkt. 15 (9th Cir. Jan. 27, 2017). Now more than ever, it is important for a retailer to make sure its cyber insurance policy covers the most significant forms of damages that stem from data breaches.

Retailers' purported obligations in the payment card landscape

Merchants typically do not process credit card payments on their own. They usually contract with third-party "servicers" who handle the credit card transactions by acting as an intermediary with credit-card-issuing banks. In turn, the servicers contract with the major credit card brands like Visa and MasterCard in order to process the appropriate credit cards. (Other card brands often contract directly with the retailer.) As part of those servicer/association contracts between the processors and the card brands, the third-party servicing companies agree to indemnify the credit card associations for certain fees and assessments resulting from a payment card information theft. Indemnity kicks in even if the incident was at the retailer level, and not on the processor's systems. These payments include reimbursement for fraudulent charges resulting from the incident and the cost of issuing new credit cards to individuals whose payment card information was compromised, or was at risk of being compromised, as part of the cyberattack. The processors then frequently demand indemnification from the retailers/merchants for the fraudulent charges and card replacement costs. Rather than demand payment, processors often take the money from the retailer by diverting funds to a reserve account that otherwise would go to the retailer for each sale.

What losses should cyber insurance cover for retailers?

In the specific context of cyberattacks involving payment card numbers,

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

RELATED TOPICS

Credit Card Risks
cyber insurance
retailers

retailers buying cyber insurance should consider whether the insurance policy provides financial protection for the following losses:

1. Breach response and investigation: Costs of forensic investigators including Payment Card Industry Forensic Investigators (PFIs), public relations firms, consumer notification letters, complying with regulatory investigations and other matters, and credit monitoring
2. Fraudulent charges and payment card replacement costs: Liabilities to payment card brands and payment card processors that issued payment cards for (a) fraudulent charges card purportedly calculated as resulting from the cyberattack, (b) operational reimbursement/costs to reissue cards, and (c) case management fees
3. Class actions: Defense costs (and settlement costs, if appropriate) for consumer and issuing bank class actions
4. Fines and penalties: Liabilities (one time or on a monthly basis) imposed due to a finding of noncompliance with payment card industry data security standards (PCI DSS compliance) and regulatory liabilities

Often, category No. 3 accounts for the lion's share of the total damages associated with a data breach. Thus, it is crucial to have a cyber insurance policy that will cover those losses in full.

Does cyber insurance cover amounts owed to card brands?

The *P.F. Chang's* decision is a red flag to cyber insurance buyers. The court ruled that although some costs were covered, such as losses in category No. 1, liabilities to the card brands and processor (category No. 3) were not. If insurance carriers rely upon this decision, claims adjusters will deny coverage under cyber insurance policies for this category of damages, unless the policy clearly provides such coverage. In *P.F. Chang's*, the company entered into an agreement with a payment card processor to process payment card transactions. Chang's used point of sale devices to send payment card information to a clearinghouse, after which the processor would credit Chang's account for the amount of the payment. The contract with the processor provided that if there was a cyberattack, Chang's agreed to reimburse the processor for "fees," "fines," "penalties," or "assessments" imposed on the processor by the payment card associations.

Thus, Chang's agreed to compensate the processor for any category No. 3 damages incurred as a result of a cyberattack. To protect itself against losses resulting from a cyberattack, Chang's had purchased a cyber insurance policy from Chubb. Chang's suffered a cyberattack on June 10, 2014, that compromised approximately 60,000 payment card numbers. As a result of the incident, MasterCard imposed assessments on the processor totaling more than $1.7 million – the majority of which consisted of a "fraud recovery assessment" for the costs of notifying affected individuals and delivering new credit cards. Chang's then sought indemnification from Chubb under its cyber insurance policy. The first insuring clause of the Chubb policy, which should have provided coverage for category No. 2 losses (third-party liability), covered loss arising out of a "privacy injury" defined as "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record, or exceeding access to such Person's Record."

Chang's asserted that the liabilities to the card brands and processor were within the scope of this third-party liability coverage. The *P.F. Chang's* court

disagreed. It found that such coverage did not apply because the processor did not sustain a privacy injury itself. The court chose not to focus on whether there was injury because of access to a person's record. Rather, it focused on the "such person's record" language and noted that the processor's records were not accessed in the cyberattack. Thus, because the processor's records were not compromised, the processor could not have suffered a privacy injury, and coverage did not apply. This part of the decision should be seen as in conflict with other third-party liability coverage decisions finding that the claimant need not be the party that suffered the loss.

There are numerous decisions interpreting liability insurance policies with similar "because of" language, and holding that the use of "because of" means the claimant itself did not have to suffer the disputed injury. It is not clear whether the policyholder asserted that the "because of" language should have governed the inquiry here. The second insuring agreement in the Chubb cyber insurance policy provided coverage for notification costs, losses that could fit into category No. 1. The court ruled that as a matter of law that the costs of card replacements fell within the second insuring agreement. The court also ruled that Chang's might be able to prove that the MasterCard management fee was a form of extra expense under the Chubb cyber insurance policy, but that it could not decide the issue on a motion for summary judgment.

The *P.F. Chang's* court also held that two exclusions barred recovery for fees passed through the processor. The policy excluded "liability assumed by any Insured under any contract or agreement" and "costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any Insured." The *P.F. Chang's* court found that those exclusions effectively "bar coverage for contractual obligations an insured assumes with a third-party outside of the Policy." The *P.F. Chang's* court decided that amounts owed to the processor and card brands were liabilities assumed under contract, and, therefore, subject to those exclusions.

The court rejected Chang's arguments that the losses should be seen as a form of equitable subrogation or based on the claim that Chang's would have been liable for the fees regardless of the contractual assumptions. The court also rejected Chang's reasonable-expectation argument that because the reason retailers buy cyber insurance is to get coverage for such fees/assessments, the court's interpretation of the policy would negate the benefit of the bargain. Given that Chang's was paying hundreds of thousands of dollars per year for the cyber policy, it is easy to understand why it would have believed that it was receiving coverage for what generally represents the largest category of damages following a cyberattack.

That said, the court explained that the record was devoid of any evidence that Chang's expected the cyber insurance policy to provide such coverage. Ultimately, the parties settled their dispute during a mediation while Chang's appeal to the U.S. Court of Appeals for the Ninth Circuit was pending. Although it is an unpublished opinion from a single court, with an appeal that was dismissed by stipulation, *P.F. Chang's* represents a stark reminder that a best practice is to review cyber insurance policies with an eye toward the known expected damages that result from a data breach. What was at issue here was a cyber policy that could be mistaken for insurance covering fraudulent charges and payment card replacement costs that are passed down by credit card issuers through the processors – but the court held that it wasn't.

Buy a cyber insurance policy carefully in the wake of the *P.F. Chang's* decision

Under *P.F. Chang's*, the policy form sold by Chubb does not cover an insured retailer's indemnification liability to a processor arising from a theft of the processor's data where the retailer is the portal through which the theft occurs. Yet this unpublished decision – correct or not – provides a roadmap for buying policies that cover a retailer's most significant damages exposure. First, brokers and underwriters should explain whether the cyber insurance policy provides specific coverage for so-called "PCI" (payment card industry) losses. The insurance company may be able to provide a policy with a definition of loss or damages to include specifically those amounts owed for operational fraud, operational reimbursement, and other amounts owed under a merchant services agreement. Certain cyber insurance policies include this language within their definitions of loss or damages in the basic third-party liability insuring agreement.

Other cyber insurance policies include a coverage section specific to PCI losses. Another alternative that certain insurance companies provide is to have so-called PCI coverage added by endorsement, specifically referring to amounts owed under a merchant services agreement. Second, if the cyber insurance policy provides some form of PCI coverage, policyholders should be aware of any sublimits on the coverage. A sublimit means that less than the full policy limit is available for particular losses. Third, policyholders should make certain that exclusions for liabilities assumed under contract either are deleted or have exceptions for liabilities under merchant services agreements. If the policy Chubb sold P.F. Chang's had included an exception for such instances, the policyholder's liability to MasterCard might have been covered in the eyes of the Arizona court.