JENNER&BLOCK

July 2016

Vol. 3, Issue 7

Insurance Law Update

Pitfalls for Data Breach Coverage under Cybersecurity Insurance Policies

By: Daniel A. Johnson

PRACTICAL POLICYHOLDER ADVICE

Many companies have recently experienced data breaches resulting in disclosure of their customers' personal or financial information. Insurers have begun offering "cybersecurity" policies that are marketed as covering such cyber risks. Policyholders, however, must be vigilant to prevent a "disconnect" between the policy as marketed and the actual policy language called upon to pay a cyber claim. To avoid any alleged "gaps" in coverage, companies should make sure that their expectations for coverage are effectively communicated to the insurer and accurately reflected in the policy's wording.

P.F. Chang's, a well-known restaurant chain, recently discovered that its cybersecurity policy would not cover various costs for remedying a data breach even though the policy was marketed as providing comprehensive coverage for cybersecurity risks. In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, No. CV-15-01322, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016), the court granted the insurer's motion for summary judgment, filed by Federal Insurance Company. While this is among the first cases to address the responsiveness of a cyber policy to a data breach, the opinion serves as a warning to policyholders that wish to obtain truly comprehensive cybersecurity coverage for all costs resulting from a data breach.

The coverage claim arose after computer hackers accessed Chang's records and obtained approximately 60,000 credit card numbers belonging to its customers. *Id.* at *4. Chang's quickly provided notice of the breach to Federal under "a CyberSecurity by Chubb Policy." *Id.* at *2, *4. Federal reimbursed more than $1,700,000 for expenses associated with the breach, including costs for forensic investigations and lawsuits, *id.* at *5, but refused to pay an additional $1,929,921.57 assessed against Chang's by its processor for credit card transactions, Bank of America Merchant Services (BAMS). *Id.* at *3.

Under the agreement between Chang's and BAMS, Chang's delivered information about customers' credit cards to BAMS, which then settled the transaction through an automated clearinghouse and credited Chang's with the amount of the payment. *Id.* The agreement also obligated Chang's to indemnify BAMS against certain fees and assessments imposed on BAMS by credit card associations like Visa and MasterCard for costs associated with data breaches. Here, MasterCard imposed three charges on BAMS that Chang's was contractually required to indemnify: (1) $1,716,798.85 for payments MasterCard made for fraudulent transaction; (2) $163,122.72 for costs to notify cardholders; and (3) a "Case Management Fee" of $50,000, which apparently was a flat fee for MasterCard's work on the incident. *Id.* at *5–6.

After receiving BAMS' request for reimbursement, Chang's requested coverage for the fees and assessments from Federal under three coverage clauses in its cybersecurity policy. Federal denied coverage, and as a result, Chang's sued Federal. Following discovery, including a deposition of the Federal underwriter, Federal filed its motion for summary judgment in which it argued that it had no obligations under the three coverage clauses, and that coverage was barred under the policy's definition of "Loss" and two exclusions barring coverage.

The first coverage clause examined by the district court promised that Federal would pay for the insured's loss due to a claim "for an Injury," including a "Privacy Injury," which the policy 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." *Id.* at *12 (emphasis added). Construing this language, the district court held that "[t]he usage of the word 'such' means that only the Person whose Record [i.e., information] is actually or potentially accessed without authorization suffers a Privacy Injury." *Id.* at *14–15. The court reasoned that a "Privacy Injury" was suffered by banks that issued the relevant credit cards because the credit card information belonged to those banks. *Id.* The court further reasoned, however, that BAMS did *not* suffer a "Privacy Injury" when it paid the banks to alleviate their "Privacy Injury," because the credit card information did not belong to BAMS. *Id.* Thus, the court concluded there was no coverage because BAMS—not the banks—was bringing the claim to pay for the banks' underlying "Privacy Injury." *Id.*

This holding is unfortunate because it arbitrarily hinges on *which entity* is seeking payment for costs associated with the underlying "Privacy Injury." Specifically, the holding implies there *would* be coverage if the issuing banks had simply imposed the same assessments directly on Chang's rather than first imposing them on BAMS, which then passed the cost on to Chang's. Nevertheless, Chang's is ultimately responsible for the same underlying "Privacy Injury" to the banks, so that there should be coverage either way. Moreover, the court never identifies anything in the policy explicitly requiring the "Privacy Injury" to have been suffered directly by BAMS. Rather, the policy only requires a claim "for an Injury," which can easily be construed as including BAMS' claim against Chang's to pay for the underlying "Privacy Injury" suffered by the banks.

As for the second coverage clause, Federal promised that it would pay for "Privacy Notification Expenses"—e.g., costs for notifying cardholders—that were "incurred by an Insured." *Id.* at *15–16. The parties disputed whether the term "incurred by an Insured" included the charges imposed by MasterCard on BAMS, which it ultimately passed on to Chang's. *Id.* On this issue, and pursuant to well-established principles of insurance contract construction, the district court held in favor of Chang's, because Chang's was ultimately liable for paying the expenses under its agreement with BAMS. *Id.* at *17–18.

Under the third coverage clause, Federal was to pay for "Extra Expenses" incurred by an insured to avoid impairment of its operations as a result of a data breach. *Id.* at *18. Chang's argued that this coverage encompassed MasterCard's "Case Management Fee" of $50,000. After finding that the Case Management Fee qualified as an Extra Expense under the Federal policy, the court ultimately denied Federal's request for summary judgment because the court could not determine whether this covered "Loss" was paid during the "Period of Recovery of Services," as required under the policy, which was an issue of disputed fact.

Because of its mixed decision on the coverage clauses, the district court then analyzed whether coverage was precluded by any exclusions or other provisions. The court held that two exclusions and the definition of "Loss" effectively barred coverage for any liabilities that Chang's "voluntarily" assumed. *Id.* at *21–22. For example, the "contractual liability" exclusion, which is commonly found in liability policies, stated that the insurer would not be liable for a loss "based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement." *Id.* at *21–22.

The court rejected Chang's argument that such provisions should not apply to obligations the insured was responsible for absent any assumption of liability, finding that there was no evidence that Chang's would have been liable to pay the MasterCard assessments to BAMS absent Chang's contractual agreement with BAMS. *Id. at *25.* In reaching this conclusion, however, the Court did not appear to conduct any detailed analysis of equitable subrogation or other legal theories under which Chang's may have been exposed to the same liability. Moreover, the court did not engage in a detailed analysis of whether these exclusions were improperly asserted by Federal to gut coverage, even though the court stated in *dicta* that it was following the black-letter rule that exclusions should be interpreted narrowly against the insurer. As a result, the opinion should be read as having very limited (if any) value as persuasive precedent on this issue.

Finally, Chang's made an argument based on the "reasonable expectations" doctrine, which under Arizona law results in a finding of coverage if (1) the insured's expectations of coverage are "objectively reasonable" and (2) the insurer "had reason to believe that the [insured] would not have purchased the . . . policy if [the insured] had known that [the policy] included" the problematic provision. *Id.* at *25–26. In support, Chang's focused on evidence that Federal knew that BAMS would recoup its losses in the event of a data breach, and emphasized that the policy was marketed as addressing the "full breadth" of technology risks. *Id.* at *27. The court rejected this argument, however, because there was no evidence that "during the underwriting process Chang's expected that coverage would exist for Assessments following a hypothetical data breach." *Id.* at *28.

Chang's has filed a notice of appeal with the U.S. Court of Appeals for the Ninth Circuit, so it may yet be reversed. Nevertheless, the trial court's decision is problematic for several reasons, not the least of which is the obvious disconnect between Federal's marketing of the policy as providing broad and comprehensive coverage and its more limited response when actually affording coverage for all costs resulting from a data breach. If policyholders want broad and comprehensive cyber policies, they would be well advised to make certain that the insurer's underwriter removes or revises any boilerplate exclusions that could effectively gut coverage for common cyber risks and their resulting costs and expenses.

Daniel A. Johnson would like to thank Matthew L. Jacobs (partner, Washington, DC) for his contributions to this article.

This Update was also published in the Los Angeles and San Francisco Daily Journal as part of Jenner & Block's monthly Insurance Law Update series.

Contact Us

Daniel A. Johnson
Associate

Phone: 212 407-1731
Email: djohnson@jenner.com
Download V-Card

Matthew L. Jacobs
Partner

Phone: 202 639-6096
Email: mjacobs@jenner.com
Download V-Card