Lessons Learned on Insuring Cyber Risk from P.F. Chang's and State Bank of Bellingham: What to Look for in Placing Dedicated Network Security/Privacy Liability Insurance

July 11, 2016 Micah Skidmore

PRACTICES Healthcare Transactions and Regulatory, Privacy and Cybersecurity, Insurance Recovery

With ever-increasing malware, spear phishing and ransomware attacks on corporate America and ever-contracting terms insuring "cyber" liability under traditional insurance, more and more risk managers are venturing into the market for dedicated network security and privacy liability or "cyber" insurance. Others remain dubious—preferring "traditional" coverage to policies that are little understood and even less tested by claims. Over the past several weeks, two judicial decisions have been issued addressing coverage for cyber risk under "traditional" and "cyber" policies. The score for policyholders: cyber insurance: 0; traditional insurance: 1.

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*, a federal district court judge in Arizona denied P.F. Chang's coverage under a specialized "CyberSecurity" policy for its liability for more than $1.9 million in credit card "assessments," representing the cost of fraudulent charges paid by Visa and MasterCard after hackers obtained some 60,000 credit card numbers from restaurant customers in 2014. Based on the contractual relationships between the relevant parties, Visa and MasterCard claimed the assessments first from card-processor Bank of America Merchant Services ("**BAMS**"), who in turn sought contractual indemnification from P.F. Chang's. According to the Court, P.F. Chang's was not entitled to payment for the assessments because the CyberSecurity policy's coverage was limited to "Privacy Injury," "sustained by a person because of actual or potential unauthorized access to such Person's Record . . . ." Because "BAMS did not sustain a Privacy Injury itself," its claim against P.F. Chang's did not trigger the policy's coverage. Moreover, according to the court, two separate exclusions for "liability assumed by any Insured under any contract or agreement" and "expenses incurred to perform any obligation assumed by, or on behalf of, or with the consent of any Insured," independently relieved Federal of any obligation to pay the assessments claimed against P.F. Chang's.

By comparison, in *State Bank of Bellingham v. BancInsure, Inc.*, a federal appeals panel affirmed summary judgment in favor of a bank seeking coverage for two fraudulent wire transfers, totaling $485,000, under a financial institution bond. Overruling arguments by BancInsure that the loss was not covered because of "employee-caused loss exclusions," the panel concluded that the "overriding cause" of the loss was "criminal activity"—not the employees' violations of policies and procedures. Based on Minnesota's "concurrent-causation" doctrine, State Bank of Bellingham was entitled to payment for its loss, notwithstanding the employees' negligent actions and their role in the loss, because "an illegal wire transfer is not a 'foreseeable and natural consequence' of the employees' failure to follow proper computer security policies, procedures and protocols."

Judging by these results, risk managers may question the necessity of so-called dedicated "cyber" insurance and find validation in reliance on "traditional" policies. In fact, while traditional coverage may provide an important source of recovery for loss and liability arising out of a data breach and should never be overlooked, the same can be said for "cyber" coverage when properly underwritten

and negotiated. Some network security/privacy liability forms are very good. Others are awful. Although each policy is different, common issues arise. Here are five items, among many others, that should be carefully considered when negotiating and placing "cyber" insurance:

1. **Trigger of Coverage**. Every insurance policy has a trigger. It could be a "claim," "occurrence," "injury," "damage" or other term. It is the event that justifies the application of a specific policy among others issued to an insured. The policy's trigger is a critically important term because it also often defines the limits and sublimits payable by the insurer as well as the retentions, deductibles and notification obligations owed by the policyholder. Due to the delays that frequently occur in discovering a data breach and the difficulty in documenting the mechanics of a breach, if the trigger is defined in terms of injury or the exfiltration of data from an insured, it may be difficult for the insured to comply with notice obligations, and disputes may arise over the number of SIRs or deductibles owed before coverage attaches. To avoid these issues, careful consideration should be given to the policy's trigger of coverage and its impact on notice, limits, SIRs and deductibles.

2. **Who is Insured?** Related to the "trigger" issue is the question, "who is insured"? Liability and even first-party coverages will apply to claims against, conduct of, and loss sustained by an "insured." Those individuals described in the definition of "insured" should include anyone within the insured organization responsible for network security, whether classified as employees or independent contractors. The "wrongful acts" that trigger liability coverage should be broadly stated to include conduct, not only by an "insured," but also anyone for whom the insured may be liable or a service provider or contractor responsible for the insured's computer systems, networks or website. When a third-party service provider is insured under your policy, or when you are an additional insured under a third-party's policy, be sure to obtain and document the appropriate waivers of subrogation from the counterparty's insurer.

3. **Definition of "Loss" or "Damages."** Covered "loss" or "damages" should include amounts paid as defense costs, settlements, judgments, pre- and post-judgment interest. "Damages" should also include fee awards. Most policies exclude fines and penalties from covered "loss" or "damages"; although, penalties ordered to be paid under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health ("**HITECH**") Act, the Gramm-Leach-Bliley Act ("**GLBA**"), state privacy laws or similar laws, rules and regulations should be included, to the extent insurable under applicable law that most favors coverage for such damages. Retailers exposed to potential card brand assessments, of the kind addressed in *P.F. Chang's*, should also seek coverage for fines and penalties assessed by card brands. To the extent that plaintiffs in a data breach scenario may seek some form of prophylactic relief, *i.e.*, credit monitoring or replacement cards, the definition of "loss" or "damages" should be correspondingly broad.

4. **Insured v. Insured Exclusions.** A relic of traditional D&O and professional liability policies, many network security and privacy liability forms will exclude loss arising from claims brought or maintained by or on behalf of an "insured." Policyholders should be vigilant to ensure that "insured v. insured" exclusions in network and privacy liability policies do not apply, *e.g.*, to (**1**) derivative claims brought without the active assistance of individual insureds; (**2**) claims brought by employees alleging the disclosure of employees' personal information; (**3**) claims brought by a bankruptcy trustee, examiner, debtor in possession, receiver or creditors' committee, without limiting the exception to claims brought in a "bankruptcy proceeding"; and (**4**) claims brought by an insured person in the form of a cross-claim or third-party claim for

contribution or indemnity which is part of, and results directly from, an otherwise covered claim.

5. **Breach of Contract Exclusions.** Borrowing from provisions in D&O and professional liability coverage, network and privacy liability policies frequently exclude coverage for loss arising from claims for or arising out of any contractual liability or obligation assumed by the insured or from a breach of contract. As a rule, these exclusions should not apply to the extent that the insured would have been liable in the absence of such contract or agreement. Because claims from customers (or employees) arising from either a network or privacy breach may ultimately be rooted in a contract or agreement, policies with "breach of contract" exclusions should include appropriate exceptions to preserve this coverage. Moreover, to avoid the result in *P.F. Chang's*, other exceptions, including preserving coverage for liability assumed under designated "insured contracts," may be appropriate for some policyholders.

Other common policy terms, too numerous to mention, including insuring agreements, arbitration provisions, defense and settlement clauses, and conduct exclusions, also deserve careful review and adjustment at times. By being attuned to these issues during the underwriting and negotiation of network security and privacy liability insurance, policyholders will be more likely to maximize recovery in the event of a breach, and "cyber" insurance will justifiably take its place among other "traditional" policies relied upon by corporate risk managers.

If you have questions about network security/privacy liability insurance or "traditional" coverage for a data breach, please contact one of Haynes Boone's insurance recovery partners listed below.