COVINGTON

Recent Cases Highlight Potential Pitfalls of New Cyber Insurance Products

June 14, 2016

Insurance

Two recent litigation developments involving cyber insurance serve as a useful reminder to policyholders: a cyber policy purchase can be full of traps for the unwary. This alert discusses the traps that resulted in one company losing coverage for a major portion of its losses from a payment card data breach, while another company faces a lawsuit by its cyber insurer seeking to void its policy. It also offers practical tips to avoid these traps.

P.F. Chang's: A Tricky Definition, a Broad Contract Exclusion, and No "PCI" Coverage Result in Incomplete Protection for Data Breach

Data breaches suffered by retailers and other businesses that handle payment cards can result in substantial assessments by card brands such as MasterCard and Visa. Retailers typically do not process payment card transactions directly with the banks that issue their customers' cards. Instead, they contract with an intermediary—called an acquiring or servicing bank—to process their customers' card transactions with the card-issuing banks. In the event of a payment card data breach, the card brands typically impose assessments on the retailer's acquiring bank, which in turn pursues indemnification under its service contract with the retailer.

That was the situation in *P.F. Chang's v. Federal Insurance Co*,[1] in which a federal district court recently held that Chang's had no cyber coverage for over $1.9 million in credit card assessments that it had to pay as a result of a data breach. The *Chang's* court found that the Federal cyber policy's "Privacy Injury" coverage did not respond to an acquiring bank's claim against Chang's for reimbursement of card brand assessments, because the Federal policy's definition of "Privacy Injury" required that the compromised confidential records at issue be the claimant's. As is typical, the payment card information stolen by the hackers belonged to Chang's customers and the card-issuing banks, not the acquiring bank that made the actual claim for reimbursement by Chang's.

To make matters worse for Chang's, the court found that Federal's contractual liability exclusion applied to otherwise covered aspects of the acquiring bank's underlying claim. The exclusion lacked customary carve-outs, and the court hewed strictly to the policy language excluding liability that the insured "assumed . . . under any contract or agreement." The court ruled that this language barred coverage because Chang's liability arose from an indemnification agreement with its acquiring bank.

[1] *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *1 (D. Ariz. May 31, 2016).

Notably, Chang's policy did not include Payment Card Industry ("PCI") coverage, a common coverage option found in cyber policies for retailers and other entities that handle payment card data. PCI coverage expressly insures amounts assessed by the card brands in the event of a data breach.

Although Federal had marketed its cyber policy as "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 "[c]overs direct loss, legal liability, and consequential loss resulting from cyber security breaches," the *Chang's* court was unmoved by arguments based upon the insured's reasonable expectations of coverage. Because Chang's and Federal were deemed to be "sophisticated parties well versed in negotiating contractual claims," the court held that Chang's reasonable expectations were confined to what was spelled out in the actual policy.

Cottage Health: Purported Misstatements in Cyber Policy Application Result in Coverage Denial for Data Breach

Cyber insurers commonly require insureds to complete detailed applications, often including extensive technical disclosure and risk self-assessments. The complaint recently filed by the insurer in *Columbia Casualty Co. v. Cottage Health System*[2] illustrates the pitfalls in these requirements.

Cottage Health, an operator of a hospital network, suffered a data breach in 2013 resulting in thousands of its patients' private medical information being publicly disclosed. In addition to other losses, Cottage Health paid $4.125 million to settle a putative class action in 2014 and faces additional proceedings arising from the breach. Columbia's lawsuit denies all coverage for the breach and seeks to rescind its policy due to the insured's alleged failure to comply with the cybersecurity practices described in its application.

In its complaint Columbia contends, first, that the "Failure to Follow Minimum Required Practices" exclusion in its cyber policy—applying to losses from, among other things, the Insured's failure "to continuously implement the procedures and risk controls identified in the Insured's application"—precludes coverage for Cottage Health's losses.

Columbia further contends that it has a right to void its policy altogether due to alleged misstatements in the "Risk Control Self Assessment" that Cottage Health completed as part of its cyber insurance application. For example, Columbia alleges that Cottage Health misrepresented:

- "that it replaced factory default settings to ensure that its information security systems were securely configured";
- "that it regularly checked and maintained security patches on its systems"; and
- "the degree of due diligence Cottage exercised with respect to [its information security management vendor's] safeguards."

[2] Complaint in Columbia Cas. Co. v. Cottage Health Sys., No. 2:16-cv-03759 (C.D. Cal. filed May 31, 2016), available at https://www.insideprivacy.com/wp-content/uploads/sites/6/2016/06/CNA-v-Cottage-Health-2016-complaint.pdf.

Relying on its broadly worded "Application" condition and "Minimum Required Practices" warranty, Columbia asserts that even if Cottage Health did not intend to deceive, a negligent misrepresentation or omission of material fact is enough under these clauses for Columbia to deem its cyber policy "null and void."

Lessons for Policyholders

Cyber insurance has become an essential line of coverage for many businesses, particularly those that handle payment card transactions or keep confidential personal health or other sensitive data. But the *Chang's* and *Cottage Health* cases are cautionary tales: a cyber insurance purchase requires both expertise and care. Cyber policy language is not standardized and requires expert scrutiny for hidden booby traps or coverage gaps. And the cyber insurance application process and its relation to policy conditions and exclusions must be managed with care, not only to avoid potential misstatements and omissions, but also to close off potential opportunities for the insurer to engage in "post-loss underwriting" by searching for inaccurate application responses—even those innocently made—to support a denial of coverage.

The adverse decision in *Chang's* might have been avoided if the insured had purchased PCI coverage and negotiated appropriate carve-outs to an unusually broad contractual liability exclusion. And Cottage Health might have avoided its dispute with Columbia if the policy's potentially onerous "Failure to Follow Minimum Required Practices" exclusion had been modified or deleted. Similarly, the policy's onerous "Application" and "Minimum Required Practices" clauses might have been moderated—for example, by limiting the right of rescission to cases of intentional misrepresentation of material fact.

Policyholder counsel at Covington frequently help clients spot potential defects and gaps in cyber wordings—before they purchase the coverage—and devise enhancements to align those wordings more appropriately with the insured's potential cyber exposures and reasonable expectations. We bring to bear our experience handling coverage claims for some of the largest data breaches in history and also work with our counterparts in the firm's Data Privacy and Cybersecurity group, who are experienced in advising clients on preventing and responding to all kinds of cyber incidents. Applying our cross-disciplinary expertise, our lawyers can help clients navigate the potentially dangerous waters of the cyber insurance underwriting and claims process.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Insurance practice group:

John Buchanan	+1 202 662 5366	jbuchanan@cov.com
Benjamin Duke	+1 212 841 1072	pbduke@cov.com
Scott Levitt	+1 202 662 5661	slevitt@cov.com
Bert Wells	+1 212 841 1074	bwells@cov.com