Who Hacked My Cyber Insurance Policy?

Title and Settlement Companies Must Know Their Risks and Their Coverage

BY ANDREW AGATI AND DEREK DIAZ

Hardly a day goes by without news of some new cyber attack. Less reported—but equally as concerning—are coverage denials under cyber-insurance policies for losses that were plainly caused by computer hackers. Here are some examples, and the lessons that can be learned from them.

Case #1: P.F. Chang's China Bistro, Inc. v. Federal Ins. Co., 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016)

P.F. Chang's purchased a "CyberSecurity" policy, which had been marketed 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."

Yet, the restaurant had no coverage for the seven-figure assessment it was charged by a credit card processing company as a result of a data breach involving the theft of 60,000 of its customers' credit card numbers. The court found that had P.F. Chang's "wanted coverage for this Assessment, it could have bargained for that coverage." While the restaurant argued that it had "expected" this type of coverage when it made its purchase, the court concluded the insured was "merely attempt[ing] to cobble together such an expectation after the fact."

There was no evidence that, during the underwriting process, the insured raised the possibility of this type of coverage in a "hypothetical data breach" and no evidence that the insured's broker "asked [the] underwriter if such Assessment would be covered."

- **The Lessons**
  - Know Your Risks: Yes, all companies face cyber risks, but you have to do your own critical risk assessment to identify precisely what risks you face and then seek out the corresponding coverage.
  - Know the Policy: Do not rely on advertising materials and the puffery that comes with it. The actual policy language will control.

Case #2: Aqua Star (USA) Corp. v. Admiralty Island Fisheries, Inc., 2016 U.S. Dist. LEXIS 88985 (W.D. Wash. July 8, 2016)

The insured purchased a "Wrap + Crime Policy" that provided coverage for the loss of money "directly caused by Computer Fraud." A hacker gained access to the computer systems of the insured's main supplier, and then began to monitor email traffic between the supplier and the insured's treasury manager.

At some point, the hacker began to intercept real emails, and then "spoofed" the treasurer by sending emails that looked as if they were coming from the supplier. Those emails directed the treasurer to change the bank account information for future wire transfers, and predictably, over $700,000 was ultimately sent to the fraudulent bank account.

The court concluded there was no coverage because of an exclusion that precluded coverage for losses "directly or indirectly" caused by "the input of Electronic Data by a natural person having authority to enter the Insured's Computer System." According to the court, this exclusion was triggered because, upon receiving the fraudulent emails, the treasury manager first updated an internal Excel spreadsheet with the "new" bank account information and then

relied on that spreadsheet in making the transfers. In effect, because the Excel spreadsheet had not been "hacked," there was no coverage.

- **The Lesson**
  - Know the Issues: This case exemplifies the type of technical coverage issues insurers will raise and that you need to be aware of before making any cyber insurance purchase. As the next case demonstrates, more favorable language could have probably been negotiated for this type of cyber risk.

Case #3: Principle Solutions Group LLC v. Ironshore Indemnity, Inc., 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016) [Motion for Reconsideration Pending]

The insured purchased a "Commercial Crime Policy," which provided coverage for "Computer and Funds Transfer Fraud." The insured sought coverage after suffering a $1.7 million loss from a computer fraud scheme. The insured's controller had received an email appearing to have come from the corporate email address of one of the insured's directors. That email informed the controller that a confidential acquisition was being planned and that an attorney would be contacting the controller to provide wire transfer instructions to complete the acquisition.

The fictitious attorney later contacted the controller, who then initiated the wire transfer. Before releasing the wire, the bank called the controller to verify how the attorney had received the wire instructions. The controller called back the bogus attorney, who advised that the insured's director had given him the information. The controller provided that information to the bank, which then released the funds.

The insurer denied coverage, arguing that: (1) the loss was not "directly" caused by the initial fraudulent email, but because of the later verbal confirmation the controller gave the bank to release the funds; and (2) the insured could have purchased an endorsement for "Cyber Deception Coverage."

The court disagreed, first ruling that the endorsement was irrelevant

since it was not part of the policy. As for the insurer's "direct" loss argument, the court held that "[i]f some employee interaction between the fraud and the loss was sufficient to allow Defendant to be relieved from paying . . . the [coverage] provision would be rendered almost pointless and would result in illusory coverage." Although ultimately siding with the insured, the court did state that the insurer's interpretation, which would require an "immediate link between the injury and its cause," was reasonable.

- **The Lessons**
  - Know the Market: While the insured in this case has not yet been tripped up by failing to buy "Cyber Deception Coverage," had the insured made that purchase from the beginning, it would have avoided the time, expense and uncertainty of coverage litigation.
  - Know the Issues: Like the insurer in Aqua Star, the insurer here was raising a "direct" loss argument. For those who have dealt with fidelity or financial institution bond policies, this is not anything new. It is far beyond the scope of this article to discuss the implications of that argument and how different jurisdictions treat it differently. Suffice it to say, however, this "direct" loss issue will likely continue to be a coverage dispute that cyber insurers will raise. Additionally, carriers are pushing back against coverage under "standard" crime/computer fraud policies for so-called "social engineering" losses, which arise when a cyber criminal dupes an employee into transferring funds. According to the carriers, a recent case, *Apache Corp. v. Great American Ins. Co.*, 2016 WL 6090901 (5th Cir. 2016), confirms their position. And so, while you could monitor future case law developments, your time and money might be better spent buying a policy that provides "social engineering" coverage.

While you could monitor future case law developments, your time and money might be better spent buying a policy that provides "social engineering" coverage.

Conclusion

For these insureds, who either did not obtain coverage or had to fight to get coverage, they may have felt like they got hacked twice: first by an Internet criminal and then, by a coverage denial that obliterated the policy and left them wondering whether they really bought cyber insurance coverage. With the lessons described above, however, it does not have to be that way for you. ■

Andrew Agati and **Derek Diaz** are partners with the law firm Hahn, Loeser & Parks LLP. The information provided is not intended to serve as legal advice. Any views expressed herein are those of the authors only. Andrew and Derek can be reached at 216-621-0150, or their respective emails, *aagati@hahnlaw.com* and *ddiaz@hahnlaw.com*.