Lowenstein Sandler

Insurance Recovery

October 19, 2021

Riding the Wave of Cyber Insurance Claim Payments: A Trend Cresting or Crashing?

By Lynda A. Bennett and Michael J. Scales

Ransomware attacks are on the rise. Cyber criminals continue to exploit lax security measures, which have become more acute in the work-from-home environment, and hack into companies' systems, encrypt their data, and then demand multimillion-dollar ransoms. Though cyber insurance policies are designed to cover these losses, insurers have responded to the increasing size and frequency of these attacks by increasing premiums, skyrocketing self-insured retentions, narrowing policy terms, and more recently, advancing coverage defenses to avoid claim payments.

A case pending in a California federal court illustrates how insurers are changing their attitudes toward these claims. In *Boardriders, Inc. v. Great American Insurance Company* (C.D. Cal., Docket Number 8:21-cv-1260), Boardriders Inc. (the parent company to apparel brands Billabong and Quiksilver) sought coverage under its cyber policy following a 2019 ransomware attack in which hackers shut down the company's networks and demanded nearly $25 million for the decryption keys. Boardriders contends that although it immediately tendered the claim to its insurer and expected immediate assistance, the insurer engaged in delay tactics by demanding detailed information and took eight months to issue a coverage position. Left without the cyber extortion coverage it expected to have readily available, Boardriders opted to try to restore its data from backups and incurred significant losses during the months it was locked out of its systems. Though the insurer eventually did make payments totaling about $5.6 million, it is now taking the remarkable position that it never owed that money and is seeking to recoup most of it by arguing Boardriders failed to prove the losses were caused by the ransomware attack. The insurer also has tried improperly to squeeze Boardriders' business interruption losses into a two-day window, despite the policy's 120-day indemnity period.

This case will be interesting to follow for a number of reasons.

First, it signifies a shift away from the response that most policyholders have received in the immediate aftermath of a breach and extortion demand where the insurer steps up and partners with the policyholder to negotiate the demand and get systems back up and running as soon as possible. The enormity and frequency of ransomware attacks has led insurers to start taking more entrenched positions on these claims and, on more recent renewals, to start placing sublimits on the amount of coverage provided for the highest risk factor cyber claims. To date, there has been little case law interpreting the terms of dedicated cyber policies because those claims have largely been paid. As such, the *Boardriders* case may provide some critical insights into how courts are going to react to insurers that do not pay on claims that are supposed to be covered by this niche insurance product.

Second, some of the grounds for the insurer's refusal to pay in *Boardriders* reflect a sign of the times and, depending on the outcome of this case, may portend changing policy language on cyber coverage forms. The insurer here relies on language that limits business interruption coverage to those losses "caused ***directly*** and ***solely*** by" the cyber incident and argues that outside factors such as the COVID-19 pandemic contributed to the losses. The insurer here is even seeking to claw back payments it previously made under a reservation of rights. Policyholders can expect insurers to make similar causation

arguments if their policies contain this language and would be well advised to engage forensic accountants to help prepare their losses in a manner that is well documented and aligns with the coverage provided under the policy. Further, if the insurer's causation argument "sticks," then policyholders will need to keep careful eyes on their renewal quotations, as cyber insurers may look to narrow their coverage obligations.

Third, this case serves as an important reminder that policyholders should take care to keep insurers informed from Day One forward after a breach has occurred and take all reasonable steps to fully document the loss. Putting insurers on immediate notice of the breach, keeping them informed about vendor engagement, and looping them in on forensic investigations, remedial action plans, and government regulatory response plans will take another insurer favorite coverage defense–lack of consent–off the table.

In sum, this case marks a shift in how insurers are treating cyber claims. While they previously worked hand in hand with policyholders and routinely paid claims, they are now fighting claims and placing the burden on policyholders from the outset, ultimately forcing policyholders to deal with devastating ransomware attacks on their own. This case could serve as a bellwether for future cyber coverage disputes, and policyholders should keep an eye on the court's decisions.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

LYNDA A. BENNETT
Partner
Chair, Insurance Recovery
T: 973.597.6338
lbennett@lowenstein.com

MICHAEL J. SCALES
Associate
T: 973.422.6770
mscales@lowenstein.com