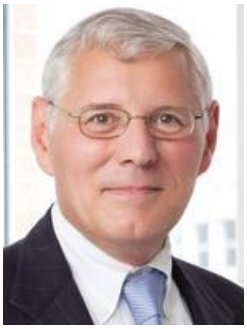
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Developing Trends In Cyberinsurance Litigation: Part 1

Law360, New York (February 10, 2017, 11:52 AM EST) --


Thomas Rohback

One of the greatest and fastest growing risks facing individuals and businesses over the last few years is the risk of some type of cyberattack or data breach. In 2013, some estimated cybercrime to cost the U.S. as much as $100 billion per year.[1] This number has ballooned, and by 2016, some estimates placed the number at $500 billion or more.[2] As reported by Forbes, "[f]rom 2013 to 2015 the cybercrime costs quadrupled, and it looks like there will be about quadrupling from 2015 to 2019."[3] To guard against this risk, companies have been buying cyberinsurance; and insurance companies have been creating and selling these policies. Today, cyberinsurance is the insurance industry's fastest growing product and it is expected to reach $7.5 billion in annual sales by 2020.[4]


Patricia Carreiro

Notwithstanding this growth, there has been relatively little litigated liability involving insurance coverage for cyberattacks and data breaches. And the insurance underwriting this relatively new risk has a very limited history on which to calculate future exposure. Although the number of law suits has grown rapidly over the past few years, the overall recoveries have been limited, particularly in instances where there has been some type of access to personally identifiable information without any actual or proven use of such information. Nevertheless, it is predicted that the number of cyberattacks, the magnitude of those attacks, and the liability springing from those incidents is going to skyrocket in the next year or two. When this occurs, companies will turn to their insurers for coverage (or face ruin). And those insurance companies that have enjoyed the inflow of premium dollars, but have miscalculated the risk, will fight to deny coverage (or face ruin). In short, the next year or two will see the birth of massive insurance coverage litigation that will dwarf the litigation spike seen several decades ago regarding "pollution exclusion" clauses. It is with this backdrop of impending Armageddon that we now turn to the otherwise hum-drum issue of insurance coverage.

Cyberinsurance Litigation Thus Far

So far, most of the insurance coverage litigation following cyberattacks or data breaches has not arisen under cyberinsurance policies but has called upon more traditional policies. Indeed, there have been only a handful of coverage cases involving cyberinsurance policies to date. But given the recent flood of different cyberinsurance policies on the market and the large number of traditional policies containing cyberexclusions, we can expect that future litigation will increasingly implicate cyberinsurance policies.

In Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs. Inc., 103 F.Supp.3d 1297 (D. Utah 2015), a

Travelers CyberFirst policy including a technology errors and omissions liability provision was litigated. The facts of this case, however, had little bearing on the unique issues of cybercoverage. There, a gym, Global Fitness, contracted with a data processing, storing and transmitting company, Federal Recovery Acceptance Inc. (FRA), to process and transfer Global's members' information. At some point, Global and FRA got into a contract dispute over failure to make payments. FRA refused to return Global's membership data until FRA was paid. Global sued FRA for the recovery of its electronically stored data and FRA sought coverage under its cyberpolicy's technology errors and omissions liability form for "errors and omissions wrongful act." The policy defined a "wrongful act" as "any error, omission or negligent act." Travelers sought a declaratory judgment of no coverage because the policy did not cover the insured's intentional acts. The court agreed. In the context of cyberinsurance, this case is significant — for its lack of significance. The subtle and esoteric issues of cyberinsurance are never triggered, and the decision sheds little light on the sophisticated coverage issues yet to come. This case could have involved FRA refusing to return a treadmill to Global Fitness until its bill was paid.

In P.F. Chang's China Bistro Inc. v. Fed. Insurance Co., No. CV-15-01322, 2016 WL 3055111 (D. Ariz. May 31, 2016), appeal docketed, No. 16-16141 (9th Cir. June 28, 2016), Chang's payment card processor, BAMS, was hacked, resulting in credit card issuer penalties against BAMS; Chang's was contractually obligated to reimburse these penalties and sought coverage from Chubb under a number of different provisions of its cybersecurity policy. Two of the insuring clauses covered losses from privacy injuries caused by "actual or potential unauthorized access to such Person's record, or exceeding access to such Person's Record," under which Chang's sought coverage for some assessments paid to MasterCard as a result of the hack. The parties, however, clashed over whether BAMS, and ultimately Chang's, could allege a privacy injury. The court held that only the individual consumers whose payment card information was stolen suffered a privacy injury, not the holders of those consumers' information. Thus, while the insurer had covered claims brought by the insured's injured customers, it was correct to deny coverage of the MasterCard assessments.

The third insuring clause at issue in Chang's covered extra expenses paid during a system recovery period due to "actual or potential impairment or denial of Operations resulting directly from Fraudulent Access or Transmission." Chang's sought coverage under this provision for a case management fee it paid BAMS to prevent BAMS from terminating its credit card processing agreement with Chang's after the breach. The insurer argued that Chang's had not shown that the breach caused actual or potential impairment or denial of Chang's business activities. The court, however, found that if Chang's had not paid the fee, Chang's would have temporarily lost the ability to process payment card transactions — a substantial part of its payments and thus a potential impairment to Chang's business. The insurer also argued that Chang's did not incur this expense during the appropriate system recovery period (ending when its system was restored from the breach), rather, the expense was incurred "nearly a year after it discovered the data breach." Chang's, however, argued that its system was still not fully restored from the breach. The court found it inappropriate on a motion for summary judgment to determine when, if ever, the Chang's system was restored. If this view is followed, we can expect future cybercoverage cases to require trials on the merits regarding the recovery period, rather than summary judgment dispositions based on contract/policy interpretation. In addition to factual issues identifying the recovery period on the back end of an event, there may also be disputed questions of fact regarding when a data breach should have been discovered on the front end.

Next, the Chang's court addressed three exclusions it called functionally identical "in that they bar coverage for contractual obligations an insured assumes with a third-party outside of the Policy." The court, drawing from the reasoning of traditional CGL policies, held that these exclusions barred coverage. Chang's argued for coverage under the "reasonable expectation" of coverage doctrine which

requires: (1) the insured had an objectively reasonable expectation of coverage; and (2) the insurer "'had reason to believe that the [insured] would not have purchased the ... policy if they had known that it included' the complained of provision." Although the court rejected Chang's argument based on its failure to show its actual expectations and based on the sophistication of both parties, it may be a doctrine that arises in future cyberinsurance coverage litigation. To prepare for this, parties should document their understandings and expectations as they negotiate for coverage and review their contracts for provisions that may void the insurance coverage they seek.

Part 2 of this article will follow tomorrow.

—By Thomas Rohback and Patricia Carreiro, Axinn Veltrop and Harkrider LLP

Thomas Rohback is a partner with Axinn Veltrop and Harkrider LLP in the firm's Connecticut and New York offices. Patricia Carreiro is an associate at the firm's Connecticut office.

[1] Siobhan Gorman, Annual U.S. Cybercrime Costs Estimated at $100 Billion, THE WALL STREET JOURNAL (Jul. 22, 2013, 6:49 PM), http://www.wsj.com/articles/SB10001424127887324328904578621880966242990

[2] Steve Morgan, Cyber Crime Costs Projected To Reach $2 Trillion by 2019, FORBES (Jan. 17, 2016, 11:01 AM), http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#58bf2a883bb0

[3] Id.

[4] PwC, Insurance 20/20 and beyond: Reaping the dividends of cyber resilience, at 4 (2015), http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.
