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

Questions Following 2 Recent Cyber Insurance Developments

By **Huiyi Chen and David Kroeger** (March 22, 2021, 4:22 PM EDT)

Huiyi Chen

David Kroeger

The cyber insurance market is getting hotter and harder.

A recent report published by MarketsandMarkets Research Private Ltd. predicts that "[t]he global cyber insurance market size in the post-COVID-19 scenario is projected to grow from USD 7.8 billion in 2020 to USD 20.4 billion by 2025, at a CAGR of 21.2% during the forecast period."[1]

Meanwhile, an increasing number of cyber incidents and a greater reliance on computers and networks in the current work-from-home environment means that large entities with significant and complex risks are facing a hardening cyber insurance market, with premiums increasing and capacity more limited.[2]

Facing the fast-growing cyber insurance market, legislatures have realized the need for greater regulation and standardization over underwriting and claims practices. Courts have also started to tackle issues specific to cyber insurance coverage — years after the first wave of major cyber incidents hit U.S. companies and consumers.

As illustrated by two recent developments in the judicial and legislative branches of government, there is still a long way to go before policyholders can expect more certainty and uniformity in the burgeoning territory of cyber insurance regulation and policy interpretation.

A Case Study and Its Implications for Cyber Insurance Law

On Feb. 8, the U.S. District Court for the District of Minnesota granted summary judgment in favor of the insurers, ACE American Insurance Company and ACE Property & Casualty Insurance Co., in litigation brought by the insured, Target Corp.[3] The court's ruling, which was decided under Minnesota law, leaves Target responsible for an unspecified but significant amount of liability, potentially in the tens of millions of dollars.[4]

The lawsuit followed one of the first known cyber incidents to affect a large portion of the U.S. population. In December 2013, Target became a victim of a massive data breach where 40 million payment card credentials and 70 million customer records stored on its systems were compromised.[5]

Like many corporate victims of cyber incidents, Target not only had to deal with breach investigation and remediation, but also faced a number of lawsuits brought by affected consumers and other third parties. The price tag of the data breach for Target was approximately $292 million in total.[6]

Among the plaintiffs that brought lawsuits against Target were a class of issuing banks which had to cancel and replace physical payment cards in the immediate aftermath of the data breach, for fear of transaction fraud resulting from the leak of cardholder and payment information.

In May 2016, Target reached settlements with the issuing banks totaling $138 million.[7] On Nov. 15, 2019, Target sued its insurer, ACE, seeking a declaratory judgment that Target's liability for the amount of the settlements allocated to the payment card replacement costs was covered under ACE's commercial general liability policies.[8] The parties filed cross motions for summary judgment in mid-2020.

When reading the over 150 pages of briefs submitted by both parties, one would think, whichever way the decision would come out, it would be groundbreaking in terms of insurance policy interpretation for cyber incidents — especially the interpretation of property or liability policies that provide coverage for losses resulting from cyber incidents.

The parties spent a great majority of the briefs on three interesting (and some may characterize as philosophical) issues:

- Whether the loss of use was caused by an occurrence (defined broadly as an accident under the policies), when the replacement of payment cards was a deliberate and intentional act by the issuing banks;

- Whether there is a distinction between "loss of use" and "loss of value" under the CGL policies, and if so, which category the replacement payment cards fall under; and

- Whether coverage for loss of use includes only the temporary damages associated with the period that the use of the property is lost, but not permanent replacement cost.[9]

The CGL policies at issue provided insurance coverage for "'ultimate net loss' ... because of 'bodily injury' or 'property damage.'"[10] The policies also defined "property damage" to include "[l]oss of use of tangible property that is not physically injured," and further provided that "[a]ll such loss of use shall be deemed to occur at the time of the 'occurrence' that caused it."[11]

Both parties agreed that the payment cards at issue here were tangible property that is not physically injured,[12] but they disputed, among other things, whether the credit cards at issue suffered a loss of use and whether the loss of use was caused by an occurrence.

One focal point of the parties' briefs was whether the loss of use was caused by an occurrence. ACE's argument was simple: The card replacement that was the subject matter of the settlement amount at issue was not caused by an accident within the definition of "occurrence" under the policies, but rather was a deliberate action undertaken by the issuing banks.[13]

Target, on the other hand, countered that the replacement of payment cards was caused by the data breach and Target's alleged negligence did not constitute an intervening cause that negated the

accidental nature of the data breach.[14]

The parties also disputed whether there was a loss of use. Target relied heavily on the U.S. Court of Appeals for the Eighth Circuit's decision in Eyeblaster Inc. v. Federal Insurance Co. in 2010, and argued that there was a loss of use because the physical payment cards were to "provide the cardholder (and only the cardholder) safe and secure access to financial accounts."[15]

When the cardholder and payment information was leaked, the physical payment cards were like "[a] front-door lock whose key has been copied and distributed among the town's criminals," which "can still be 'locked' with the key, but the lock has 'lost its use' as an object that protects the home from intruders and must be replaced."[16]

ACE countered that the physical payment cards could still be used as intended by cardholders for transactions in person or online, but their value diminished because the data breach enabled cyber thieves to commit fraudulent transactions using the leaked payment information stored on the physical cards.[17]

ACE used the lock-key analogy against Target by arguing "[w]hen its owner loses exclusive control of a lock's key, the lock does not lose its ability to function as a lock. It loses its value as a lock. However, loss of use coverage requires a loss of use in fact, not merely in value."[18]

ACE also advanced an argument in support of its position that loss-of-use damages are time-based under Minnesota law.[19] It quoted a Minnesota Supreme Court decision that stated "[w]hen a chattel is damaged, not amounting to total destruction in value, the damages include compensation for loss of use."[20]

According to ACE, the damages resulting from the loss of use could include rental costs for a substitute or lost profits when the property was temporarily down, but would not include replacement costs for property that was totally destroyed.[21]

Target refuted ACE's argument based on the plain reading of the policy language, which did not include any temporal restrictions to the loss of use, and similarly distinguished a flurry of Minnesota and out-of-state case law that ACE relied upon for its temporal argument.[22]

During oral argument, the court and the parties continued to focus on these key issues, especially the definition of "loss of use" and whether the physical credit cards at issue lost their use immediately after the data breach.

The court asked counsel for both parties questions such as:

- "So the cards were no longer trustworthy [after the data breach,] ... it is the loss of trustworthy transactions that was the loss of use; is that correct?"[23]

- "And so it is a secured purchase use that you would indicate would be the linchpin for loss of use; is that correct?"[24]

- "But isn't built within that use of a, let's say, credit card or debit card the fact that it is secured use?"[25]

At the conclusion of the oral argument, the court praised both parties' arguments as "well-developed and well-presented and clearly presented" and indicated that counsel were "very responsive to the Court's questions."[26]

However, in a 12-page order, the court did not adopt the definition of "loss of use" argued by either party — it did not adopt ACE's argument that the physical credit cards only became less desirable to use after the data breach (due to security concerns) and did not lose their use (consumers can still use them for transactions); and it also did not adopt Target's argument that the use of the physical credit cards includes an expectation for secured use, which was lost immediately after the data breach.[27]

In fact, the decision did not even discuss the different definitions that were the focus of the briefings and oral argument.[28] Instead, the court elided the "use v.s. value" debate by concluding that "[t]he facts of this case ... do not involve the value of the plastic payment cards" because "[n]o party submits that the value of the plastic payment cards diminished after the Data Breach."[29]

"As such, the question of a diminution of the value of the payment cards also is not presented."[30] The court then dismissed ACE's temporal damage argument by stating that "ACE presents no Minnesota case law holding that loss-of-use damages are exclusively time-based."[31]

Surprisingly, the court's decision in favor of ACE was based on a theory that neither party appears to have focused on in briefings or oral argument — i.e., that of causation.

The court seized on the causation requirement for loss-of-use damages in cases cited by the parties on the temporal damage issue — an issue the court summarily dismissed — and held that the loss of use of the payment cards was not based on the data breach because "the record is devoid of any allegation or evidence as to what the value of the use of the payment cards is, either to Target's customers or to the payment card companies," and "as the value of the use is not established or even approximated ... damages cannot be 'based on' the loss of use because there is no nexus between the damages and the loss of use."[32]

As a result, "the connection between the damages claimed and the loss of use of the payment cards is insufficiently direct and, therefore, the damages claimed are not loss-of-use damages covered under the [p]olicies."[33]

As to whether the loss was caused by an occurrence, the court decided that it need not resort to case law that discussed the definitions of an occurrence because Target did not satisfy the causation element discussed above.[34]

The Target decision and its reasoning thus leaves more puzzles than it resolves.

As discussed above, ACE explicitly argued that the payment cards' value diminished after the data breach, and used the lock-key analogy to illustrate why (i.e., the cardholder lost the exclusive control of the data associated with the plastic payment cards), and it is unclear why the court wrote "[n]o party submits that the value of the plastic payment cards diminished after the Data Breach."[35]

In addition, the court's holding seems to suggest that the evaluation of damages (i.e., "what the value of the use of the payment cards is") is a condition precedent to proving causation (i.e., the payment cards replacement costs were "based on" the loss of use of the payment cards).

It is inevitable that courts will face some of the unresolved issues involved in Target in the future. Take the recent SolarWinds Corp. cyber incident as an example.

According to the FireEye report, the threat actors "gained access to numerous public and private organizations around the world ... via trojanized updates to SolarWind's Orion IT monitoring and management software. This campaign may have begun as early as Spring 2020 and is currently ongoing."[36]

The malware spies on the victims' systems and has the ability to steal data. Users who installed the trojanized software may or may not have been hacked, and nonusers may have become infected through interaction with infected users.[37]

They are facing a difficult choice between costly replacement of suspected machines/networks and the danger of being spied on and targeted for fraud or theft. The situation is thus analogous to the situation the cardholders/issuing banks faced in Target.

Although no insurance coverage litigation has been filed for losses resulting from the SolarWinds cyber incident to date,[38] one could easily foresee such lawsuits in the near future.

If the victims choose to replace the infected/suspicious machines, would the replacement costs be based on a loss of use?

Does it matter that the loss of use is permanent and not temporary?

If the victims choose to continue to use the infected/suspicious machines, do these machines lose their use or merely suffer diminution of value?

How would these issues play out under different state laws and before courts that decide to substantively address these issues?

Policyholders that seek insurance protection and risk minimization in light of the increasing number of cyber incidents are facing uncertainties regarding judicial interpretation of the insurance policies they bought (assuming they are successful in obtaining cyber coverage in a hardening market).

New York Cyber Insurance Risk Framework Could Increase Cyber Insurance Costs

The judiciary is not the only branch of government that has sought to respond to the need for more clarity and uniformity over cyber insurance practices.

On Feb. 4, the New York State Department of Financial Services issued a nonbinding framework for best practices for New York-regulated property and casualty insurers that underwrite cyber insurance.[39] The guidance was the first of its kind nationwide. It recognized the criticality of cybersecurity and cyber insurance:

> From the rise of ransomware to the recently revealed SolarWinds-based cyber-espionage campaign, it is clear that cybersecurity is now critically important to almost every aspect of modern life—from consumer protection to national security. ... Cyber insurance plays a key role in managing and reducing cyber risk. This is a relatively new area of insurance for most insurers, but one that has grown rapidly.

The New York DFS framework is far from comprehensive — it briefly listed seven points that insurers and policyholders should be aware of:

1. Establish a Formal Cyber Insurance Risk Strategy.

2. Manage and Eliminate Exposure to Silent Cyber Insurance Risk.

3. Evaluate Systemic Risk.

4. Rigorously Measure Insured Risk.

5. Educate Insureds and Insurance Producers.

6. Obtain Cybersecurity Expertise.

7. Require Notice to Law Enforcement.[40]

Some of the recommended practices will potentially cause a potentially significant increase in costs for policyholders looking to cover cyber risks.

For example, policyholders can reasonably expect a much more rigorous and comprehensive survey by the insurer of the policyholder's cybersecurity system, "including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies," to enable the insurer to "rigorously measure insured risk."

And one can translate "obtain cybersecurity expertise" into transferring increased insurer costs to increased premiums.

A more controversial aspect of the framework is the recommendation against making ransom payments in ransomware attacks; the framework also cited potential sanctions for violations under guidance issued by the Office of Foreign Assets Control.

Paying ransom has been a remedy often resorted to by insurers and policyholders to lower the downtime caused by a ransomware attack. If they are deprived of this option, one could expect more coverage disputes arising out of, inter alia, increased costs of remediation (such as total replacement of infected machines).

It is unclear whether other states will follow suit in issuing guidance to insurers and policyholders related to cyber insurance and what form the guidance will take. More regulation does not necessarily equal greater certainty in the policyholders' favor, however, as demonstrated by the New York DFS framework.

Conclusion

From boardroom to courtroom, companies seeking to procure and establish coverage for potential or actual losses resulting from the increasing number of cyber incidents face significant uncertainties.

It is unclear how the courts around the country will interpret policy language when the damages incurred are intangible and temporary, but at the same time massive in scale and broad in the type and number of victims.

Legislative efforts to provide guidance to insurers and policyholders do not always add to certainty and clarity and may risk increasing costs (in the form of premiums or otherwise) to companies attempting to obtain coverage in a hard cyber insurance market.

Huiyi Chen is an associate at Jenner & Block LLP.

David Kroeger is a partner and co-chair of the firm's insurance recovery and counseling and reinsurance practices.

[1] See MarketsandMarkets, Cyber Insurance Market by Component (Solutions (Analytics & Cybersecurity) and Services), Type (Standalone & Packaged), Coverage (Data Breach & Cyber Liability), Organization Size, End User (Technology & Insurance), and Region - Global Forecast to 2025, available at Cyber Insurance Market Size, Share and Global Market Forecast to 2025 | MarketsandMarkets.

[2] See Bethan Moorcraft, US Cyber Insurance Market at Exciting Crossroad, Insurance Business America (Oct. 16, 2020), available at https://www.insurancebusinessmag.com/us/news/cyber/us-cyber-insurance-market-at-exciting-crossroad-236496.aspx; David Gambrill, Demystifying Cyber's First Hard Market, Canadian Underwriter (Nov. 12, 2020), available at https://www.canadianunderwriter.ca/insurance/demystifying-cybers-first-hard-market-1004199880/.

[3] Target Corp. v. ACE Am. Ins. Co., Case No. 19-cv-2916 (WMW/DTS) (D. Minn. Feb. 8, 2021), ECF No. 49 (the "Target Order").

[4] The insurance coverage action concerned a large and unspecified portion of a $138 million settlement in an underlying matter. See Target Mem. ISO Mot. for Partial Summ. J., 7, Target, Case No. 19-cv-2916 (WMW/DTS) (D. Minn. May 25, 2020), ECF No. 29 (the "Target Opening Br.").

[5] See Lysa Myers, Target Targeted: Five years on from a Breach That Shook the Cybersecurity Industry, WeLiveSecurity (Dec. 18, 2018), available at https://www.welivesecurity.com/2018/12/18/target-targeted-five-years-breach-shook-cybersecurity/.

[6] Target Opening Br., 1.

[7] Id. at 7.

[8] Target Order at 2.

[9] See generally Target Opening Br.; ACE's Opp. Mem. & ISO Cross-Mot. for Summ. J. (the "ACE Opp."), ECF No. 36; Target Resp. to ACE's Cross-Mot. for Summ. J (the "Target Resp."), ECF No. 39; and ACE's

Reply ISO Cross-Mot. for Summ. J. (the "ACE Reply"), ECF No. 42, Target, Case No. 19-cv-2916 (WMW/DTS).

[10] Target Order at 2.

[11] Id.

[12] An interesting twist, which is not at issue in the Target case, is that some property policies may define loss or damage to electronic data as a result of malware intrusion or other cyberattacks as "physical damage," and therefore provide express (and not "silent") cyber coverage.

[13] ACE Opp. at 33–38; ACE Reply at 32–34.

[14] Target Opening Br. at 11–16; Target Resp. at 32–36.

[15] Target Opening Br. at 2

[16] Id. at 2, 18–26.

[17] ACE Opp. at 2, 14–20.

[18] Id.

[19] ACE Reply at 15–21.

[20] Id. at 15 (quoting In re Commodore Hotel Fire & Explosion Cases, 324 N.W.2d 245, 250 (Minn. 1982))

[21] Id. at 15–21.

[22] Target Resp. at 19–27.

[23] Oct. 20, 2020 Hr'g Tr. at 21, Target, Case No. 19-cv-2916 (WMW/DTS).

[24] Id. at 25.

[25] Id. at 42.

[26] Id. at 51–52.

[27] See Target Order at 6–8.

[28] See id.

[29] Id. at 8.

[30] Id.

[31] Id.

[32] Id. at 11.

[33] Id. at 12.

[34] Id. at 6.

[35] Id. at 8.

[36] FireEye, Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor (Dec. 13, 2020), available at https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

[37] See Tony Howlett, Best of 2020: The SolarWinds Supply Chain Hack: What You Need to Know, Security Boulevard (Dec. 24, 2020), available at https://securityboulevard.com/2020/12/the-solarwinds-supply-chain-hack-what-you-need-to-know/.

[38] Based on a docket search as of March 19, 2021.

[39] New York DFS, SUPERINTENDENT LACEWELL ANNOUNCES DFS ISSUES CYBERSECURITY INSURANCE RISK FRAMEWORK, Press Release (Feb. 4, 2021), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202102041.

[40] New York DFS Cyber Insurance Risk Framework (Feb. 4, 2021), available at https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.