PLI Chronicle

May 2022

A Fast-Moving Topic: Cyber Coverage in 2022

Joshua Gold

Daniel J. Healy

Anderson Kill, P.C.

Cyber risks are the fastest evolving risks faced by policyholders. Seemingly every day, new risks emerge, new attack vectors are honed, and new scams are discovered by organizations of all sizes and across all industries. A number of insurance coverage developments have taken place over the past several months, and lessons learned from these developments can help policyholders address existing and new cyber perils. Awareness of these insurance coverage issues also can help avoid or at least resolve coverage disputes.

Cyber risks have been found to be covered by dedicated cyber policies and more traditional lines of coverage. The fact that losses involve a computer system breach should not automatically negate coverage under insurance policies. To the contrary, recent court decisions evince coverage under D&O, crime, property and general liability insurance policies. Numerous court rulings support policyholder positions that such insurance policies provide coverage for at least some components of the losses typically suffered from a cyber incident. The following discussion addresses some key developments about which policyholders at risk of a possible cyberattack should be mindful.

Data Breach Is Not Exclusively a Cyber Policy Issue

A breach of a computer network or device can lead to a number of different forms of loss, especially when customer financial data is involved. A policyholder may be

faced with compliance issues, notification requirements as to all affected customers, data integrity issues, ongoing data breach issues, litigation risks, and losses from fraudulent use of the compromised data, among other things. Not surprisingly, the range of losses may not fit neatly within a single cyber policy. In particular, policyholders have successfully pursued coverage for data losses and security related losses under Commercial General Liability policies.

For example, in July 2021, the U.S. Court of Appeals for the Fifth Circuit reversed a trial court decision, finding coverage for a payment card data breach in *Landry's Inc. v. Insurance Co. of the State of Pennsylvania*. There, Landry's sought coverage for a data breach that resulted in thousands of customers' payment card information being stolen after a hacker stole the payment card information from a number of Landry's retail locations. The theft led to Landry's merchant bank, Paymentech, seeking to hold Landry's liable for fraudulent use of the stolen payment card information, alleging more than $20 million of losses. The merchant bank suit against Landry's stemmed from a Visa and MasterCard assessment of damages against it for fraud charges and replacement expenses stemming from the hack.

Landry's argued that it was expressly promised CGL coverage for the underlying merchant bank complaint because Paymentech was seeking damages that fell within the CGL policy coverage. Landry's pointed to the coverage grant in the policy that extended to losses "arising out of . . . [the] [o]ral or written publication . . . of material that violates a person's right of privacy." The insurance company denied coverage, arguing that no "publication" took place from the theft.

The Fifth Circuit held that the theft involved publication and was covered. It stated, "The Paymentech complaint plainly alleges that Landry's published its customers' credit-card information—that is, exposed it to view."

Given that the policy plainly covered liability arising from violations of consumers' privacy rights, the Fifth Circuit also rejected the insurance company's "salami-slicing distinctions" as to the nature of the complaint (alleging breach of contract as opposed to tort).

More recently, in March 2022, a federal trial court judge in *Target Corporation v. ACE American Ins. Co.*, reversing her own prior decision, held that CGL insurance covered payment card replacement costs after the financial information underpinning those payment cards was compromised through a breach in network security. The *Target* decision and the *Landry's* decision demonstrate the applicability of CGL coverage to evolving cyber risks.

Data Loss and Data Compromise Coverage

Property policies can also provide coverage for cyber losses. In a now well-known decision, the federal district court in Maryland found coverage for data loss under a property policy in January 2020 in *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co*. The policyholder there suffered a ransomware attack that rendered software, as opposed to the policyholder's computer hardware, less operable. Following the attack, the system lost functionality and operated more slowly than previously.

The policy in *National Ink* provided property coverage for

(a) Electronic data processing, recording or storage media such as films, tapes, discs, drums or cells;

(b) Data stored on such media

Homing in on the policy language, the court determined that term "data" was qualified with the phrase "stored on such media," making clear that the policy provided coverage for the data itself. The decision further clarifies that coverage under non-cyber policies plainly applies to cyber loses.

That decision has been cited by other decisions finding first-party coverage for cyber-related losses. This year, an appellate court in Ohio held that a policyholder could recover for cyber losses under a property policy. Last November, in *EMOI Services, LLC v. Owners Ins. Co.*, the court rejected the insurance company's argument seeking dismissal of the policyholder's claim for coverage. The insurance company argued that the policyholder could not demonstrate sufficient direct physical loss, including because the losses involved software damage in a ransomware attack. Pointing to deposition testimony from the policyholder's software developer and IT manager asserting that the attack damaged the company's software and data, the court rejected the conclusion that such loss could not be covered under a property policy. The property insurance company has since appealed that case to the Ohio Supreme Court.

Loss of Money

In some circumstances, including ransomware and phishing attacks, part of the loss consists of theft, including via ransom or fraud-induced transfer of funds. The monetary portion of a cyber loss—meaning loss via theft as opposed to the costs of incurred through repair or liability—may be disclaimed by an insurance company (even one promising robust cyber insurance protection). Thus, crime insurance may play an important role here. Despite this, some commercial crime insurance companies fight

against providing coverage for cyber-related thefts of funds, but policyholders should not assume denials under crime policies are correct.

For example, in the *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.* case decided last year by the Indiana Supreme Court, the court ruled crime insurance could provide coverage for a ransomware payment but that discovery was needed to determine whether there was indeed coverage. In that case, Continental Western Insurance Co. denied coverage for a ransomware attack in which the policyholder paid the ransom and did not regain its full functionality in its computer system. Continental contended that the policy "specifically excluded" computer hacking and computer virus coverage because the policyholder had declined to purchase a computer hacking and computer virus coverage extension—a so-called "Agribusiness Property and Income Coverages" policy extension. Continental also contended that the policyholder had voluntarily transferred the ransom payment and therefore it was "not" a theft of funds essentially.

By sending the case back to develop the actual facts of the ransomware hack, the decision acknowledges that even without the specific cyber coverage extension, the crime policy at issue potentially provides coverage for G&G's ransomware loss. Emphasizing that point, the Supreme Court of Indiana stated at the outset of its coverage analysis that it does "not believe G&G Oil's declination of computer virus and hacking elsewhere in the Policy is dispositive of this claim."

Biometric Losses

Statutes driving biometric data-related liabilities have made headlines in recent years. While the alleged liabilities are based on statutes that have, in a number of cases, been on the books for years, it is the evolving security environment that has given rise to more claims in recent days. Biometric data is used with much greater regularity and, thus, stored at much higher rates resulting in increased allegations of statutory violations governing biometric data and security.

Insurance companies have cited exclusions intended to apply to federal telecommunications statutes to support their denial of coverage for liabilities incurred under Illinois's Biometric Information Privacy Act, commonly called "BIPA." The exclusions in question typically bar coverage for claims asserted under the Telephone Consumer Protection Act (TCPA) or the CAN-SPAM Act of 2003. These types of exclusions will sometimes reference any other statute that is similar to the TCPA and CAN-SPAM Act.

Fortunately for policyholders, the Supreme Court of Illinois has held that this kind of exclusionary language did not apply to BIPA. In *West Bend Mutual Insurance*

Company, v. Krishna Schaumburg Tan, Inc., for example, the insurance company sued for a declaration that BIPA claims against its policyholder were barred from coverage based on this form of exclusion. West Bend argued that BIPA's regulation of the use and storage of biometric information was similar to the TCPA's regulation of telephone calls and faxes and the CAN-SPAM Act's regulation of e-mails. The Illinois Supreme Court applied the well-recognized doctrine of *ejusdem generis* to find that BIPA was not the same kind of statute and, instead, required the insurance company to provide defense coverage to the policyholder.

The Illinois Supreme Court decision carries great weight in this area given that BIPA is an Illinois statute and many other states have predicated their regulation of biometric data on BIPA. Already this year, a federal court in Illinois followed the approach laid out in *Krishna* when another insurance company sued its policyholder for a declaration of no coverage for BIPA claims. In *Citizens Insurance Company of America v. Wynndalco Enterprises, LLC*, the insurance company also claimed the TCPA/CAN-SPAM Act exclusion applied to BIPA. Rejecting the insurance company's arguments, the Illinois federal court held that "the Statutory Violation exclusion is intractably ambiguous." Just this past March, in *Citizens Insurance Company of America v. Thermoflex Waukegan, LLC*, the U.S. District Court for the Northern District in Illinois, considering a similar exclusion, held that BIPA is not a statute of the same kind as the TCPA, the CAN-SPAM Act, or the FCRA—or, at least, it is unclear whether BIPA is like enough to those other statutes to be corralled in a catch-all clause excluding coverage for "any other statute" broadly similar to those named.

Nonetheless, a federal district court for the Middle District of North Carolina reached a contrary decision last year. The court undertook to apply the "main purpose" of the exclusion, rather than the specific words of the exclusion, and concluded that the main purpose was to exclude coverage for statutes that protect and govern privacy interests in personal information.

Policyholders should seek coverage for potential BIPA liability under all applicable policies, including general liability policies, and be prepared to push back against denials that may be without proper legal basis. The *Krishna* decision should be persuasive outside of Illinois, as BIPA is the leading statute and other state laws are based upon it.

Labels Do Not Control Coverage

As the foregoing recent decisions from state and federal courts demonstrate, policy language and the facts of a loss are of key importance. Labels and insurance industry lingo are not.

Many policyholders have heard the term "silent cyber" tossed around. Some underwriters use the term to refer to ostensibly "surprise" coverage under non-cyber policies that applies to any portion of a loss that involves any cyber-related incident. The term is in essence insurance industry spin. The traditional policies (whether D&O, E&O, General Liability/CGL, crime insurance, property insurance, etc.) have provided significant coverage for policyholder losses, which increasingly involve some type of electronic hardware, media, data, software, information or other category of property. The losses may take numerous forms. In all-risk policies in particular, all coverage is in a sense silent: only exclusions are enumerated. Underwriters' attempts to rename losses fly in the face of evolving business realities.

Indeed, the *G&G* case decided last year recognized the fallacy of a concept like "silent cyber." The court acknowledged that the policyholder had refrained from purchasing a specific cyber coverage endorsement and stated that such a fact alone did not negate coverage under a commercial crime insurance policy for a cyber loss resulting from a ransomware attack.

The "war" exclusion is another defense insurance companies have deployed to deny coverage for cyberattacks. But such a defense to coverage is dubious, at best. In a December 2021 case, *Merck Co. Ins. Et al. v. ACE American Insurance Co. et al.* (published in January 2022), the New Jersey Superior Court ruled that a war exclusion did not negate insurance coverage sought by pharma giant Merck for $1.4 billion in losses stemming from a malware infection, inserted in the global NotPetya attack of 2017, that spread to 40,000 Merck computers.

NotPetya was a major global attack focused primarily on Ukraine but affecting companies worldwide. The U.S. and U.K. governments have accused Russia of helping steer the attacks. Seizing the sensational reporting on this topic, the insurance companies deemed NotPetya to be, as described in the decision, "an instrument of the Russian Federation as part of its ongoing hostilities against the nation of Ukraine."

Emphasizing that in an all-risk policy such as Merck's "the burden of proof is on the insurer to show that a policy exclusion applies," the court stated:

> Merck maintains its reasonable understanding of this exclusion involved the use of armed forces, and all of the case law on the war exclusion supports this interpretation, . . . no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein.

The decision highlights that successful denial of coverage based on the "war" exclusion requires more than industry lingo, alleged non-conventional warfare operations, and media reports.

Last, the BIPA coverage disputes have given rise to yet another insurance industry label: "the Statutory Violation Exclusion." The label is another misnomer. As explained above, the exclusion expressly applies only to certain types of statutes, namely the TCPA and the CAN-SPAM Act. While there is a provision in many of the exclusions that states the exclusion applies to other similar statutes, there is no support for the argument that the exclusion applied to all statutes regulating communications. Broad applications of exclusionary language are typically rejected under the law of most states.

As with "silent cyber" and "the war exclusion," policyholders should be wary of the insurance industry's periodic use of broad labels as if they set forth the actual scope of insurance protection. Adopting such language can create obstacles to coverage and needlessly complicate proper interpretations of insurance coverage.

Conclusion

These recent decisions provide ongoing examples of the fast-evolving nature of cyber risks that policyholders face. Policyholders will need to be prepared for new cyber perils and an increasingly challenging claims-handling landscape when they seek the insurance protection that they paid for.

For more information, check out the authors' Cyber Insurance Claims, Case Law, and Risk Management book, available from PLI Press (read now on PLUS).

Joshua Gold is a shareholder in Anderson Kill's New York office, chair of Anderson Kill's cyber insurance recovery group and co-chair of the firm's marine cargo industry group.

Daniel J. Healy is a partner in Anderson Kill's Washington, D.C. office, co-chair of the firm's cyber insurance recovery group, co-chair of the firm white-collar and regulatory practice group and a former Trial Attorney for the U.S. Department of Justice.

PLI Programs you may be interested in	PLI Press Publications you may be interested in	To submit an article for consideration, please contact the editor at editor.plichronicle@pli.edu or visit pli.edu/PLIChronicle/contribute for more information	**Sign up for a free trial of PLI PLUS at** pli.edu/pliplustrial

Disclaimer: The viewpoints expressed by the authors are their own and do not necessarily reflect the opinions, viewpoints and official policies of Practising Law Institute.

This article is published on PLI PLUS, the online research database of PLI. The entirety of the PLI Press print collection is available on PLI PLUS—including PLI's authoritative treatises, answer books, course handbooks and transcripts from our original and highly acclaimed CLE programs.