New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Insurance Law

WWW.NYLJ.COM

VOLUME 266—NO. 66

MONDAY, OCTOBER 4, 2021

# Cyber Insurance Coverage for **Breach of Privacy** Claims: The Law Is Evolving

**BY JOSHUA GOLD AND DENNIS NOLAN**

© ADOBE STOCK

Organizations in various industries have faced a spate of third-party demands and claims after computer network data has been exposed, whether inadvertently or deliberately, via data theft. In the wake of compromised health information, payment card information, or other sensitive data, organizations often hear from regulators and sometimes law enforcement. Civil litigation represents a definite possibility, too. Many companies will face a barrage of lawsuits and even class action litigation where sensitive data has been stolen or disclosed improperly. Those class actions have had more teeth and more staying power in recent years. Recently, Zoom reportedly agreed to pay $85 million and bolster its security to resolve class action privacy litigation pending in California.

Many policyholders facing this kind of litigation exposure rightly look to their liability insurance for protection, including not only dedicated cyber policies, but also their D&O insurance, E&O insurance, and general liability insurance (aka CGL insurance). The resulting insurance coverage battles have been hard fought in numerous jurisdictions—especially under the personal injury insuring promises of CGL insurance coverage.

The case law has evolved in recent years, particularly on the often-contested question of whether theft or accidental exposure of personal information constitutes a covered violation of privacy under CGL policies. Below, we review three influential decisions handed down between 2014 and 2021 that tackled this issue.

JOSHUA GOLD *is a shareholder in the New York office of Anderson Kill P.C. and chair of the firm's cyber insurance recovery group.* DENNIS NOLAN, *a shareholder in firm's New York office, is a member of the insurance recovery group, and, as co-chair of the firm's bankruptcy group, focuses on insurance coverage issues in Chapter 11 cases.*

### CGL Insurance Coverage for 'Personal Injury' Claims

In one of the first filed litigations for personal injury coverage under a CGL insurance policy for hacked information, a New York Supreme Court Justice presided over the question of whether there was a "publication" of private customer data that had been hacked by cyber criminals and thus violated their right to privacy. In this case, often referred to as "*Sony I*", the trial court held the policyholder had no coverage for underlying privacy litigation following a hack of a multi-tenant cloud platform. See *Zurich American Ins. Co. v. Sony Corp. of America* (N.Y. Sup. Ct. Feb. 21, 2014).

While the court found that the hack certainly constituted a "publication" of stolen electronic information, the court also held that coverage could not obtain because the policyholder had not itself published the information. Instead, the court found that the only publication of the hacked information was by the cyber crooks, and that was, in the court's view, insufficient for purposes of triggering the CGL policy's personal injury insuring provision. The court reasoned that under that policy the publication needed to be by the policyholder and not the hackers in order to be covered. The case settled before a New York appellate court ruled on the policyholder's appeal.

### A Different View From the Fourth Circuit

Two years after the *Sony I* decision, the U.S. Court of Appeals for the Fourth Circuit came to a different interpretation of personal injury coverage in a CGL policy for a data compromise lawsuit—though under somewhat different circumstances. In this case, the policyholder faced a class action suit when private patient medical information was posted and remained available on an open-facing server. The record on appeal indicated that the patient information was fully accessible through an Internet search engine query. *Travelers Indemnity Co. of America v. Portal Healthcare Solutions*, No. 14-1944 (4th Cir. April 2016). The Fourth Circuit affirmed the trial court's analysis that:

> [T]he class-action complaint "at least potentially or arguably" alleges a "publication" of private medical information by Portal that constitutes conduct covered under the Policies. See Travelers, 35 F. Supp. 3d at 771 (internal quotation marks omitted). Such conduct, if proven, would have given "unreasonable publicity to, and disclose[d] information about, patients' private lives," because any member of the public with an internet connection could have viewed the plaintiffs' private medical records during the time the records were available online.

It should be noted that in this case, the question of who published the data was not at issue, as theft of data was not involved.

### The Fifth Circuit Weighs In

This summer, another federal appellate found coverage for violation of the right of privacy, this time in a case that did involve data theft. In *Landry's v. the Insurance Co. of the State of Pennsylvania*, No. 19-20430 (5th Cir. July 21, 2021), the U.S. Court of Appeals for the Fifth Circuit presided in a coverage dispute over a CGL insurance claim made by Landry's after the theft of payment card information from its systems.

Due to the hack of payment card data, Landry's merchant bank asserted over $20 million in losses due to card brand assessments and sought to pass this liability on to Landry's, which refused to pay. After the merchant bank sued for payment, Landry's filed a claim for insurance coverage with its CGL insurance company, but the insurance company denied coverage.

The district court found in favor of the insurance company, holding that the complaint did not allege a "publication," but alleged only that a hacker penetrated the card processing system and stole credit card information, without alleging a publication that resulted in a privacy violation. The appellate panel reviewed to determine whether the underlying complaint sought damages "'arising out of

… [the] [o]ral or written publication … of material that violates a person's right of privacy'…We first determine whether the Paymentech complaint involves a 'publication.' Then we determine whether Paymentech seeks damages 'arising out of" the 'violat[ion] [of] a person's right of privacy.'" Concluding that the allegations made against the policyholder by the merchant bank were covered, the appellate panel found that there was indeed a "publication" of sensitive payment card information asserted in the underlying complaint. Specifically, the Fifth Circuit reasoned:

> The Paymentech complaint plainly alleges that Landry's published its customers' credit-card information—that is, exposed it to view. In fact, the Paymentech complaint alleges two different types of "publication." The complaint first alleges that Landry's published customers' credit-card data to hackers. Specifically, as the credit-card "data was being routed through affected systems," Landry's allegedly exposed that data—including each "cardholder name, card number, expiration date and internal verification code." Second, the Paymentech complaint alleges that hackers published the credit-card data by using it to make fraudulent purchases. Both disclosures "expos[ed] or present[ed] [the credit-card information] to view."

The Fifth Circuit panel thus cited language in the complaint that treated the theft of data as publication by Landry's *to the hackers*—a point that no doubt would have been highly relevant in challenging the outcome in *Sony I* had it made its way through the entire appellate process.

The Fifth Circuit also analyzed whether the publication of the credit card information arose out of a violation of a person's right to privacy. The Fifth Circuit found that it clearly did, given the "breadth" of the insuring provisions of the CGL policy for personal and advertising injury coverage: "Thus, the Policy does not simply extend to violations of privacy rights; the Policy instead extends to all injuries that arise out of such violations. Next, the Policy insures against 'violat[ions of] a person's right of privacy'… [T]he plain text of the Policy anticipates ICSOP's duty to defend in the Underlying Paymentech Litigation."

> The case law has evolved in recent years, particularly on the often-contested question of whether **theft or accidental exposure of personal information** constitutes a covered violation of privacy under CGL policies.

The Fifth Circuit found that it was beyond dispute that the allegations in the merchant bank's underlying lawsuit "constitute an injury arising from the violation of customers' privacy rights, as those terms are commonly understood." In considering the CGL insurance company's proposed coverage requirement of a suit sounding in tort, the panel rejected it, holding that it "does not matter that Paymentech's legal theories sound in contract rather than tort. Nor does it matter that Paymentech (rather than individual customers) sued Landry's. Paymentech's alleged injuries arise from the violations of customers' rights to keep their credit-card data private." The Fifth Circuit reversed and remanded the case, concluding that under the eight-corners rule of policy construction in Texas, the CGL insurance company "must defend Landry's in the Underlying Paymentech Litigation."

## Conclusion

Further rulings can be expected on the scope of insurance coverage for privacy claims and class actions stemming from compromises of data security.

While holdings may vary based on state insurance law considerations, different perspectives between trial courts and appellate courts, and federal court systems vs. state court systems, the extent of insurance protection for cyber class action privacy claims under liability insurance products will remain important given the scourge of data breaches.