Policyholder Wins Appeal for CGL Coverage in $20M Credit Card Cyber Data Theft Claim

This case underscores that insurance coverage for cyber claims can come under different insurance products.

By **Joshua Gold** | August 02, 2021

Underscoring that insurance coverage for cyber claims can come under different insurance products, a recent decision by the U.S. Court of Appeals for the Fifth Circuit held that the policyholder is entitled to defense coverage under a CGL policy for a $20 million lawsuit after a cyberattack grabbed payment card information from its computer systems.

In *Landry's Inc. v. the Insurance Co. of the State of Pennsylvania*, No. 19-20430 (https://casetext.com/case/landrys-inc-v-the-insurance-company-of-the-state-of-pennsylvania) (5th Cir., July 21, 2021), the Fifth Circuit reversed a trial court ruling that had favored the insurance company. Policyholder Landry's, a multi-brand restaurant and hospitality company, had been sued for more than $20 million by its merchant bank Paymentech after Visa and Mastercard had assessed damages against Paymentech for payment card fraud charges and replacement expenses stemming from a hacker's theft of payment card information at certain Landry locations.

After Visa assessed Paymentech's liability for the data breach at $12.7 million and Mastercard at $7.8 million, the merchant bank sought to pass this liability on to Landry's, which sought coverage under a CGL insurance policy. The insurance company denied coverage to Landry's.

Appellate Court Review: CGL Coverage Under "Personal Injury" Insuring Agreement for Hacked Data Damages

The policyholder asserted that it was expressly promised CGL coverage for the underlying merchant bank complaint because Paymentech was seeking damages "arising out of . . . [the] [o]ral or written publication . . . of material that violates a person's right of privacy." The insurance company fought the insurance claim on multiple grounds, including whether there was a "publication" of the sensitive payment card information that was stolen by the hackers. In finding that there was a covered publication of sensitive payment card information alleged in the underlying complaint, the Fifth Circuit explained:

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." Publish, Webster's Second, at 2005. And either one standing alone would constitute the sort of "publication" required by the Policy.

Next, the panel rejected the insurance company's argument that the CGL insurance policy's personal injury coverage was narrow in scope, holding instead that the publication of the credit card information arose out of a violation of a person's right to privacy. The Fifth Circuit found that "the Policy instead extends to all injuries that arise out of such violations." The Fifth Circuit also held that it's "undisputed that a person has a 'right of privacy' in his or her credit card data. It's also undisputed that hackers' theft of credit-card data and use of that data to make fraudulent purchases constitute 'violations' of consumers' privacy rights. And it's still further undisputed that the Paymentech [underlying] complaint alleges such theft and such fraudulent purchases. Thus, the plain text of the Policy anticipates ICSOP's duty to defend in the Underlying Paymentech Litigation."

The CGL insurance company also argued that even if there was a covered publication of stolen payment card information, insurance coverage was still not available because the personal and advertising injury coverage "only" applied to tort losses—and "not" to losses arising from a breach of contract. The Fifth Circuit rejected this argument, finding that the relevant insuring clauses did not say what the insurance company claimed they said:

ICSOP urges us not to follow the plain text of the Policy and instead to alter it. In ICSOP's view, the Policy covers only tort damages "arising out of . . . the violation of a person's right of privacy." Thus, ICSOP suggests, it might defend Landry's if it were sued in tort by the individual customers who had their credit-card data hacked and fraudulently used. But ICSOP thinks it bears no obligation to defend Landry's in a breach-of-contract action brought by Paymentech. Of course, the Policy contains none of these salami-slicing distinctions.

The panel concluded 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, finding that the CGL insurance company "must defend Landry's in the Underlying Paymentech Litigation."

Claim Notice and Risk Management Lessons

This case is a reminder that policyholders may have insurance coverage for their cyber claims under insurance products beyond just their dedicated cyber insurance policies. Further, some policyholders may have had their "personal injury" coverage moved from their CGL policies in recent years and placed, instead, into their cyber liability insuring agreements or in their E&O insurance policies.

While there is no one-size-fits-all approach for assessing where and when cyber coverage will be available, there is one universal rule when it comes to dealing with cyber-related claims: give notice across the board to every possibly implicated insurance policy. And make that notice prompt. Cyber insurance claims tend to be hard-fought, given their size, increasing frequency, and novelty, so it's best not to complicate them further by opening the door for an insurance company to exploit "late notice" arguments. Underwriters we have spoken with on panel discussions have themselves indicated that if they were in the policyholder's shoes, they would give notice broadly.

Given that case law involving cyber insurance claims is limited and does not yet give a full and clear picture of how to navigate claims and dense policy terms, policyholders should act to keep their options open when it comes to determining what policies provide what coverage for each category of loss stemming from a cyber incident.

Joshua Gold (https://andersonkill.com/People/Joshua-Gold) is a shareholder in Anderson Kill's New York office. He is chair of the Cyber Insurance Recovery Practice Group and co-chair of the Marine Cargo Insurance Group.

These views are the author's own.
