LAW360

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

The Biggest Cyber Coverage Decisions Of 2021

By **Daniel Tay**

Law360 (December 21, 2021, 5:21 PM EST) -- Case law about cyberinsurance coverage continued to rapidly evolve in 2021, with courts finding coverage for cyber incidents available under policies ranging from property to commercial crime to general liability.

As cyberattacks are projected to continue increasing in frequency, policyholders should scour all their policies, even noncyber ones, to ensure they don't leave any coverage on the table, attorneys told Law360.

Here, Law360 breaks down the biggest decisions on cyberinsurance coverage in 2021.

Landry's Panel Expands Definition of 'Publication'

The Fifth Circuit's July holding that an insurer **must defend** Landry's Inc. in a $20 million data hack dispute with JPMorgan Chase Bank boosted policyholders' hopes that such breaches, projected to continue becoming more frequent, could be covered under advertising injury provisions in commercial general liability policies.

The Fifth Circuit said in July that hackers' use of Landry's customers' credit card information fell under personal and advertising injury coverage provisions in the company's policy. (Nicolas Asfouri/AFP via Getty Images)

The two-judge appeals panel held that under the CGL policy issued to Landry's by Insurance Co. of the State of Pennsylvania, the definition of a "publication" that is covered by personal and advertising injury provisions can be broadly defined to include the passing on of information or making data publicly available.

The panel determined publication happened in two circumstances in Landry's case. The first occurred when hackers made Landry's customers' credit card information available, and the second took place when the hackers used that information to make fraudulent purchases.

The holding gives the term "publication" an expansive definition that encompasses more than what is considered publication in the traditional sense, and it rejects the notion that publication by a third party cannot trigger coverage, said Bradley Nash, a partner at Hoguet Newman Regal & Kenney LLP.

"Clients sometimes think of advertising injury as though it has to be like a publication in a newspaper, but in fact it's a much broader definition," Nash told Law360. "It's the definition that

exists in defamation law; it's really just any kind of public display."

Nash noted that in a separate case in New York state court, Zurich American Insurance Corp. v. Sony, the court had held that there was no coverage because the publication of private information had been committed by the hacker and not Sony, the policyholder. The Landry's decision, in contrast, is a "strong, pro-policyholder decision," Nash said.

Nash also said the court's holding that the disclosure of information to the hackers could be considered publication was a "watershed decision" that would be applicable in many cases.

The decision means that insurers will likely begin defining "publication" much more narrowly in their policies or begin using a different term altogether, said Avi Gesser, a partner at Debevoise & Plimpton LLP, which represents policyholders.

"I'm somewhat sympathetic to insurers on these issues because cyber risk is a very, very serious underwriting issue," Gesser told Law360. "If those kinds of risks are being put into general crime policies, or other policies that are not designed for the kind of losses that are associated with cyber or privacy instances, then they've just got a mismatch between their risk and their underwriting."

At the same time, the impact of the Landry's decision may be blunted by the fact that the case was based on an older policy, with most newer CGL policies having an exclusion for disclosure of personal information created to prevent cyber liability coverage, said Joshua Mooney of Kennedys CMK, which represents insurers.

"One, Landry's is a bit of an outlier case, notwithstanding it's the Fifth Circuit, but two, you're not even getting to that analysis because the exclusion itself would prohibit coverage," Mooney told Law360. "Policyholders have claimed that this decision signals a broadening of coverage under CGL policies, and that simply is not the case."

The case is Landry's Inc. v. Insurance Co. of the State of Pennsylvania, case number 19-20430, in the U.S. Court of Appeals for the Fifth Circuit.

Ransomware Payments May Be Covered Under Crime Policies

The Indiana Supreme Court, in reviving G&G Oil Co.'s lawsuit against its insurer, **found that ransomware payments** may be covered under computer fraud provisions in commercial crime policies. The decision bolsters the idea that ransom payments are not voluntary actions that break the causation link between a ransomware attack and a company's losses.

The court's March reversal of a trial court's ruling in favor of Continental Western Insurance Co. made it the first state high court to weigh in on coverage for ransomware under crime insurance policies. The policy issued to G&G Oil covered losses "resulting directly from the use of any computer to fraudulently cause a transfer of money," and the payments G&G Oil made undisputedly involved the use of a computer, the Indiana Supreme Court said.

The trial court's interpretation of the policy term "fraudulently cause a transfer" had been overly narrow, the high court said. The justices said the phrase should be read as "to obtain by trick." Under this interpretation, the information that the hackers needed to break into G&G Oil's computer servers and drives could have been obtained by trick, the justices said, remanding to the lower court for more fact-finding on how the hacking scheme was carried out.

"We do not think every ransomware attack is necessarily fraudulent," the justices said, noting that a hacker could access a company's network without trickery if the company did not implement an adequate security system.

The Indiana high court's decision is the first to find that ransomware payments can constitute a fraudulent payment that would be covered by a crime policy, said Jim Carter, a policyholder attorney at Blank Rome LLP. The court's holding that there was a direct link between the use of a computer and the ransomware payments was "innovative" and particularly important as insurers often challenge coverage claims based on whether there is such a link, Carter told Law360.

"What constitutes directness is not specifically defined in the policies," Carter said. The decision also was notable because the oil company had rejected coverage for computer hacking and viruses when negotiating its policy, and the court still found coverage under the policy the company did purchase, Carter said.

Another win for policyholders under the G&G Oil case is that the court rejected the argument that the payment had been made voluntarily and therefore there was no direct link or causation between the ransomware attack and the payment, said Cindy Jordano, a partner at Cohen Ziffer Frenchman & McKenna, which represents policyholders.

"It's only voluntary in the sense that they chose to do it, but really, they were under duress, it was directly caused by the ransomware attack," Jordano said.

She noted the case echoed arguments seen in the context of "spoofing" cyberattacks, or scams in which attackers disguise malicious communications as being from a trusted source. She said there had been a federal circuit court split on whether actions by affected companies' employees in the spoofing context "break the causation."

In the case of G&G Oil, the court had addressed similar causation arguments in the context of a different type of attack and come up with a decision that was a win for policyholders, Jordano said.

The case is G&G Oil Co. of Indiana v. Continental Western Insurance Co., case number 20S-PL-00617, in the Indiana Supreme Court.

Medical Biller's Hack Covered Under Property Policy

An Ohio appellate court's split ruling that EMOI Services **could potentially** be covered under a property policy for losses from a ransomware attack marked another example of how cyber coverage may be found in noncyber policies.

The court majority said in November that the medical billing company could potentially get coverage from Owners Insurance Co. after hackers encrypted its software and demanded a ransom. The panel pointed to testimony from the company's software developer and information technology manager that the hacking of EMOI's systems damaged them beyond just simply rendering files inaccessible.

EMOI's policy defined "media," for the purposes of coverage for physical loss or damage to media, as material in which information is recorded, including "computer software and reproduction of data contained on covered media." The appeals panel found the fact that the policy identified "software" and "data" means that media is not just a physical device, so damage to EMOI's software, like the hacker's encryption, could be covered.

The court's ruling is an expansion of coverage for companies without specific ransomware or cyber policies, Debevoise's Gesser said. At the same time, he cautioned that the outcomes of such cases will often turn on "very specific language in the policies."

"I think this process is going to result in much clearer guidelines in terms of what is and isn't excluded in various policies, but we're in a period of uncertainty," Gesser said, referring to the coverage of cyber incidents under provisions for physical loss or damage to media. "I don't know how common the language of EMOI is — I assume it's a fairly common formulation of a policy — and so it would not surprise me if this gets tested again."

It remains to be seen if other courts will follow the EMOI decision's reasoning, Mooney of Kennedys CMK said, or if they "are going to recognize the decision wrongfully conflated concepts of loss of use and physical damage."

"When you're in a regulated industry, you're going to deal with outlier decisions. Whether or not you should revise policy language based upon that decision is going to be dictated by whether or not other courts begin agreeing with it," he said.

The case is EMOI Services LLC v. Owners Insurance Co., case number 29128, in the Court of Appeals of Ohio for the Second Appellate District.

Opinions Diverge in BIPA Coverage Cases

Two different rulings in cases that dealt with coverage for violations of Illinois' Biometric Information Privacy Act demonstrate the importance of policy language and choice of law, attorneys told Law360.

The Illinois Supreme Court ruled in May that West Bend Mutual Insurance Co. **must defend tanning salon** Krishna Schaumburg Tan Inc. against a customer's suit alleging that the business disclosed her fingerprint data to a third-party vendor in violation of BIPA.

The high court said the business' disclosure fell within the term "publication" as used in the advertising injury provisions of the business owner's liability policy issued by West Bend. The justices rejected the insurer's argument that publication only occurs when private information is disclosed to the general public, holding that publication could be defined as disclosure to one or more individuals.

In contrast, a North Carolina federal court found in Massachusetts Bay Insurance Co. v. Impact Fulfillment Services that three Hanover liability insurers **did not need to cover** Impact, a logistics company, because an exclusion for recording and distribution of information precluded coverage for alleged BIPA violations.

While the West Bend decision was significant in that it provides a broad definition of "publication," Mooney said the exclusion at issue in that case was very narrow, highlighting how specific language in the policy is important in determining the outcomes of such coverage disputes. He said the exclusion on which the Impact case turned — the more common exclusion in currently issued CGL policies — is much broader.

"The question, in my mind, is wide open again in Illinois, and really limits West Bend to only those policies that have an older distribution of material policy exclusion," Mooney said.

The difference in the policy language in the two cases was a good example of how exclusions have to be specifically drafted and how policyholders must read their policies carefully, Cohen Ziffer's Jordano said.

"In the West Bend case, the exclusion, even though it was dealing with the same facts as the subsequent case, was not specific," she said. "Then in the Massachusetts Bay case, you have an example where you're dealing with the same facts, but a reworked exclusion where the insurance companies are much more specific about the privacy statutes that they wanted to exclude."

Still, the fact that BIPA is an Illinois statute means that West Bend, decided by the Illinois high court, is likely to be "far more influential," said Peter Halprin of Pasich LLP, which represents policyholders.

"We have that as kind of a guiding light" in Illinois, Halprin said of the case, while noting that "with the possibility of appeal out there, there's a lot of uncertainty outside of places like Illinois."

The cases are West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan Inc. et al., case number 125978, in the Illinois Supreme Court, and Massachusetts Bay Insurance Co. v. Impact Fulfillment Services, case number 1:20-cv-00926, in the U.S. District Court for the Middle District of North Carolina.

--Additional reporting by Daphne Zhang, Lauraann Wood and Shane Dilworth. Editing by Aaron Pelc.