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 State Of Cyber Coverage Law: 4 Key Decisions

By **Jeff Sistrunk**

Law360, Los Angeles (April 19, 2016, 8:53 PM ET) -- The Fourth Circuit's ruling last week that Travelers must defend Portal Healthcare against a class claim that its failure to secure a server caused a breach of its medical records added to a small but growing body of case law on insurance coverage for cyber-related claims.

Here, Law360 takes a look at the four most significant cyber coverage decisions in recent years and the potential impact of the rulings.

Travelers v. Portal Healthcare Solutions

The Fourth Circuit issued an unpublished opinion on April 11, affirming a Virginia federal court's decision that Travelers must defend Portal Healthcare Solutions LLC against a proposed class action that alleges the policyholder's failure to secure its server made medical records accessible by unauthorized users online.

The district court had found that mere availability of information online equates to a "publication" under the personal or advertising injury provision in Portal's commercial general liability policy with Travelers, thereby triggering the insurer's duty to defend. The appellate panel adopted the lower court's rationale.

The Fourth Circuit's acceptance of a broad interpretation of the policy's publication language marked a significant win for policyholders seeking coverage for data breach incidents under CGL policies, according to experts.

"There is a recognition here that once there is a disclosure of otherwise sensitive or confidential information, the genie is out of the bottle," said Josh Gold, a cyberinsurance attorney at Anderson Kill PC.

While the policyholders shouldn't abandon the notion of acquiring specialized cyber policies in the wake of the Fourth Circuit's ruling, the decision indicates that coverage may still be available for data breaches under traditional insurance, experts say.

"While there is not a guarantee of coverage under a CGL policy, the ruling gives a ray of hope to policyholders who haven't purchased standalone cyberinsurance," said Katie Varholak, a member of Sherman & Howard LLC's litigation department. "If there is a breach, policyholders may be able to find

coverage under CGL insurance."

The case is Travelers Indemnity Co. of America v. Portal Healthcare Solutions LLC, case number 14-1944, in the U.S. Court of Appeals for the Fourth Circuit.

Recall Total Information Management v. Federal Insurance Co.

In May, the Connecticut Supreme Court became the first state high court to rule on the availability of coverage for a data breach under a CGL policy, affirming a decision nixing coverage for the $6 million in losses IBM Corp. incurred in dealing with a 2007 mishap that exposed the sensitive information of 500,000 employees.

Adopting the decision of an intermediate appeals court, the Connecticut justices held that a pair of insurers didn't have to cover losses tied to an incident in which a cart holding IBM computer tapes fell out of the back of a transportation contractor's van near a highway exit ramp. About 130 of the tapes, which contained Social Security numbers, birth dates and contact information for past and present IBM employees, were removed from the road.

According to the opinion, IBM contractor Recall Total Information Management Inc., now known as Recall Holdings Ltd., and subcontractor Executive Logistics Inc. had not triggered a section of the relevant policy providing coverage for injuries caused through the publication of material that violates a person's right to privacy. There was no indication that anyone ever accessed the confidential information on the stolen tapes, the Connecticut high court found.

Insurers heralded the decision as another nail in the coffin of policyholders' efforts to seek CGL coverage for data breaches while policyholder advocates said the case could be limited by its unusual facts.

"In Recall Total, the disclosure itself was very low-tech — the case did not involve information hacked through a computer system," Gold said. "Additionally, there apparently was no irrefutable evidence that any of the information was misused."

However, facts similar to those in the Portal case are more likely to recur in future coverage disputes than those in the Recall Total case, experts say.

"I think that Portal is more of a victory for policyholders than Recall Total could be considered a defeat," said K&L Gates LLP partner Roberta Anderson.

The case is Recall Total Information Management Inc. et al. v. Federal Insurance Co. et al., case number SC19291, in the Connecticut Supreme Court.

Zurich American Insurance Co. v. Sony

The New York state judge who oversaw Sony Corp.'s now-settled dispute with its insurers over coverage for the Playstation Network cyberattack took a similar approach to the Portal court in interpreting the publication language in a CGL policy.

Judge Jeffrey K. Oing ruled from the bench in January 2014 that hackers' theft of confidential data on tens of millions of Sony PlayStation users constituted a publication of private information, as required by the entertainment giant's insurance policies with Zurich American Insurance Co. and Mitsui Sumitomo

Insurance Co. of America.

"The takeaway from both Portal and Sony is if a third party saw or could potentially see the information, there was a publication," said Barnes & Thornburg LLP partner Scott Godes.

However, Judge Oing still held that the policies' coverage for the oral or written publication of materials that violate a person's right to privacy could not be triggered through the actions of third parties, in this case, the hackers that stole confidential information from Sony's PlayStation Network.

"The court read a requirement into the policy that the publicity or disclosure be performed by the insured," Varholak said.

Sony sought appellate review of the case but settled with Zurich and Mitsui in April 2015 before the appeals court could render a decision.

While policyholders and insurers alike can still cite certain conclusions in Judge Oing's ruling, the trial court decision doesn't hold nearly as much persuasive value as an appellate court decision in the case would have, experts say.

The case is Zurich American Insurance Co. v. Sony Corp. of America et al., case number 651982/2011, in the Supreme Court of the State of New York,

Travelers v. Federal Recovery Services

In response to the proliferation of data breaches and other cyber risks, insurance companies have begun to write broad cyber exclusions into CGL policies while also rolling out a variety of cyber-specific policies. However, experts say that insurers and policyholders will continue to see coverage disputes under cyberinsurance products, as indicated by a decision in a Utah federal court case in May.

In that case, U.S. District Judge Ted Stewart ruled that Travelers had no duty to defend a pair of data processing companies under a cyber liability policy in a suit alleging they withheld customer information from Global Fitness Holdings Inc.

The district judge determined that the underlying claims weren't rooted in negligence as required by defendants Federal Recovery Services Inc. and Federal Recovery Acceptance Inc.'s CyberFirst technology errors and omissions policy with Travelers. Judge Stewart's ruling was the first substantive decision issued in a cyberinsurance coverage dispute.

"The big-picture takeaway from the case is that insurance companies are repeating over and over that policyholders should buy cyber or technology E&O insurance to cover risks relating to electronic data and computer-related liabilities," Godes said. "Here, though, the insurer sued to deny coverage nonetheless."

Global members had provided credit card and bank account information through which the gym could bill them. The fitness chain had a servicing retail installment agreement with FRA requiring the data company to process member accounts and transfer members' fees to Global, according to court documents.

After Global entered into an asset purchase agreement with LA Fitness, it notified FRA of the need to

return member account data, court papers said. The fitness chain alleged that FRA withheld portions of the data until Global satisfied several "vague demands for significant compensation."

Judge Stewart said coverage was unavailable for the data processing companies under the Travelers policy because Global didn't allege errors, omissions or negligence but rather "knowledge, willfulness and malice."

But experts say that the decision could have a limited impact because it largely rested on the particular facts of the case.

"This was another one of those unusual cyber cases in that it was largely a dispute between a policyholder and consumer, rather than a hacking or unintended disclosure situation," Gold said.

The case is Travelers Property Casualty Company of America et al. v. Federal Recovery Services et al., case number 2:14-cv-00170, in the U.S. District Court for the District of Utah.

--Editing by Christine Chun and Philip Shea.