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

Cyberattack Class Suits Have Unpredictable Insurance Impact

By **Shawn Rice**

Law360 (June 30, 2021, 5:55 PM EDT) -- Companies crippled by cyberattacks often face hefty costs to manage the fallout, but subsequent class actions over compromised data can have particularly unpredictable financial impacts on these companies and their insurers, according to legal experts.

In June, four class actions — two in federal and two in state courts — accused Scripps Health, a hospital system that was hit with a data breach during a cyberattack, of negligently handling the personal and financial information of more than 147,000 patients, staff and physicians. San Diego's second largest health care provider is blamed for failing to protect network servers, according to court records.

While many high-profile ransomware attacks involve hackers taking control over a company's computer or network, the Scripps Health incident highlighted the danger of personal information being stolen.

Andrew Lipton, vice president and head of cyber claims at AmTrust Financial Services Inc., told Law360 he was concerned with the unpredictability of third-party privacy class action claims, which can either "go the distance" and settle for tens of millions of dollars or be a "dud" and settle for far less when chances of class certification are uncertain.

Privacy class actions "are pretty new and developing at a rate that is unreal," Lipton said, comparing them to securities class actions on the directors and officers insurance side, where there is a "wealth of data" and settlement value on a case-by-case basis can be estimated based on stock price metrics.

Judy Selby of Hinshaw & Culbertson LLP, who represents insurers, also told Law360 that there was uncertainty about how these class action privacy suits will play out. When there were large retail data breaches in recent years, it was expected that a suit would follow, Selby said, but with this new crop of data breaches it isn't automatic.

"Now you work through the first-party claims and costs, and you wait to see if there is any litigation to come from it. You may have a bit of that exposure hanging out there for a while," she said.

The unpredictability of privacy class action suits with respect to exposure and damages stems from the uncertainty of class certification and potential for statutory penalties, according to legal experts.

By comparison, insurers in securities class action cases can expect most classes to be certified and settlements to amount to 10% to 15% of the damages plaintiffs seek class-wide, according to experts.

But for privacy class suits, where statutory penalties can run $5,000 per violation, legal experts feared that a large, certified class could mean very high theoretical plaintiffs' damages.

"I don't love the math," Lipton said.

While cyberattacks have been widespread across industries, dozens of hospitals large and small have been subject to attacks. The health care industry was tied for second among industries susceptible to ransomware attacks, according to data released by Fitch Ratings in May, which said attacks increased 485 percent in 2020 globally, with total global costs estimated at $20 billion.

Hospital systems especially carry a wealth of information, according to legal experts, like names, addresses, social security numbers, financial information and protected health information to entice cyber criminals.

"Hospitals do present a target rich environment," Scott C. Hecht of Stinson LLP told Law360. Stinson represents policyholders.

Michael Miguel of McKool Smith, who also represents policyholders, agreed, telling Law360 hospitals can't operate without this information and don't have the luxury to wait it out and not pay the ransom. Hackers have picked entities "with very little appetite or ability to string it out and not pay a ransom," he said.

For other legal experts, Scripps Health was an obvious target for class action litigation given the extent to which the country has gone to legislate laws for health care information protection. Both class actions cite obligations under the federal Health Information Portability and Accountability Act, according to court documents.

"If a hacker is smart enough to go in and keep a company out of their system, then you can believe they have checked out what you are capable of paying out. You get to shoot with a BB gun and not a buck shot. You can find vulnerable hospitals and other entities with information that will be volatile," Miguel said.

Legal experts said the victim-business's lost revenue and added expense can be substantial and insurable. For Scripps Health, which according to court documents suffered a partial suspension of its hospital operations due to the cyberattack, the losses should be covered, according to legal experts.

Hospital systems like Scripps Health may turn towards their cyber insurance policies to cover breaches of data security and systems security, according to experts. Assuming cyber coverage has been purchased, legal experts said the predominant challenges to companies are sublimits on coverage for particular things that are covered.

These specifics include IT forensics, legal compliance and mitigation expenses, according to experts.

"Ten years ago, most businesses didn't have dedicated cyber coverage," Hecht said. "Now, it's becoming the rule rather than the exception."

Lipton of AmTrust said it was a "growing problem" for excess cyber insurers to determine how much of the underlying limits would have been spent on the first-party claim — which can include items like business interruption losses and costs to notify customers whose data was exposed — before a

company like Scripps Health needs coverage for follow-on third-party claims. A calculation on limits can be tested when a cyberattack happens, Lipton explained.

"There is greater predictability with first-party liability with the costs. With first-party liability you are putting out the fire," Lipton said. "The third-party aspect is unpredictable."

Class privacy actions create a splash in the news as they involve sensitive information falling into a hacker's hands following a cyberattack. But legal experts said the suits raise a difficult question on proof whether a company properly safeguarded information and what that stolen information is worth.

With these class suits, legal experts said businesses will often look to shift the blame regarding the negligence that facilitated the cyberattack onto a vendor or some other third-party. And courts will need to grapple with proof of negligence in not protecting the information with the latest security technology.

"You're talking about highly sophisticated criminal activity. When something gets well-respected in the tech community, someone finds a way around it," Miguel of McKool said.

--Editing by Peter Rozovsky.
