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

How Lawyers Are Keeping Hacked Clients Out Of Court

By **Shayna Posses**

Law360, New York (June 27, 2017, 3:50 PM EDT) -- After watching the likes of Yahoo and Anthem face an onslaught of litigation upon announcing that massive breaches compromised millions of customers' information, companies may well panic at the prospect of having to disclose a data security incident. But while breaches make for splashy headlines, experts say the number of incidents that actually lead to lawsuits is fairly low.

With every entity, from small corporations to government agencies, primed to gather valuable data, no one is immune from cybersecurity incidents, BakerHostetler noted in its **2017 Data Security Incident Response Report**. However, just because incidents are sometimes unavoidable doesn't mean companies are doomed to a flood of lawsuits every time they provide notification of a breach.

Legal experts say there are plenty of things companies can do to better prepare for these incidents and mitigate the fallout when they happen, ranging from initial steps like establishing a response plan and minimizing data collection to clearly communicating with consumers after a breach and helping them navigate any potential risks.

And then there's the fact that the majority of breaches don't lead to lawsuits, no matter what the publicity of some breaches seems to suggest, experts say.

BakerHostetler clients informed customers of data security incidents 257 times in 2016, but less than 5 percent of those situations led to lawsuits, according to the report. That number has remained fairly steady over the last few years, with the firm determining that around 6 percent of the incidents it handled in both 2014 and 2015 spurred litigation.

Bryan Cave LLP has reached similar conclusions in its annual Data Breach Litigation Report, finding that about 4 percent of the breaches publicly reported between the third quarters of 2013 and 2014 and around 5 percent of those announced from the fourth quarter of 2014 to the same point in 2015 led to class action litigation.

Jena M. Valdetero, a Bryan Cave partner who heads the firm's data breach response team, said the findings are consistent with the experiences she and her colleagues have had handling breaches.

"Despite the fact that the investigations and the response are time-consuming and can be costly, usually litigation doesn't flow from them," she said. "You have to handle a breach as though you anticipate that a lawsuit would actually come, but typically — and we tell clients this — more often than not, it's not going to be the case that you get sued."

So what's the deal with the misconception that data breaches lead to a sea of suits? Law360 turned to cybersecurity experts to find out what keeps the litigation numbers low and what factors make actions more likely.

Plaintiffs Face an Uphill Battle

Data breach lawsuits present a real challenge for plaintiffs and their attorneys, experts say, deeming this one of the main reasons why the number of actions has remained low even though, according to

an Identity Theft Resource Center report, the number of breaches in the United States jumped by 40 percent last year to a record high of 1,093.

"A lot of these cases, at least the ones that we're working on, have been dismissed, and I think that probably has discouraged a lot of lawyers from jumping in and trying to get suits filed as soon as they hear about a breach," said Theodore Kobus, leader of BakerHostetler's privacy and data protection team.

Plaintiffs face a number of hurdles, chief among them establishing standing. Under the U.S. Supreme Court's landmark Spokeo decision, demonstrating concrete harm is key to showing Article III standing, but many plaintiffs leading data breach suits have struggled to convince judges that their alleged injuries are material.

In many cases, it's hard to demonstrate a sufficient connection between a breach and actual harm, said Paul Stephens, director of policy and advocacy for Privacy Rights Clearinghouse.

"How does one prove that that specific breach was the reason for the person becoming a victim of identity theft?" he said. "That's very difficult to do, particularly because the identify theft may occur years down the road."

Proving damages is a problem for the same reason, Valdetero said. With plaintiffs often alleging intangible harms like an increased risk of future identity fraud, these cases can be pretty tough to value and the damages can end up being fairly low, attorneys say.

That being said, Valdetero noted, the plaintiffs bar is continuing to evolve, asserting theories of harm that are getting some traction in the initial pleading stage, like the time and money spent closing down accounts. However, she said, there's a big difference between beating a motion to dismiss and surviving summary judgment or prevailing at trial.

That's why Edelson PC is urging the plaintiffs bar to focus on cases that invoke strong theories, where attorneys can actually secure settlements or judgments that compensate clients, founder Jay Edelson said.

For instance, some circuit courts have held that the fear of future identity theft, a popular theory in these cases, can be enough to establish sufficient harm in some circumstances. But that avenue is hurting the privacy bar, Edelson said.

That'll get a plaintiff past a motion to dismiss, but, he said, "you don't just have to show standing, you have to actually quantify damages. Under these theories, they can't do that."

A damage theory that has proven particularly successful for his firm is overpayment — alleging that when a defendant promised good security but failed to deliver, they owe consumers some of the money they paid for the company's services, Edelson said. It doesn't work in every situation, however, like when a free service is involved, he noted.

Ultimately, Valdetero said, "The law hasn't caught up with how to respond to a data breach in a way that provides relief to the affected consumers with respect to things like establishing standing and establishing damages."

Breach Targets Getting Savvier

Companies and other entities that collect sensitive data are also getting better at preparing for and managing incidents, including being more proactive about offering services to help mitigate the impact, all of which contributes to minimizing the number of actions, the BakerHostetler report said.

After seeing others bungle breach responses, companies are learning lessons, hiring experienced lawyers, putting response plans in place and taking time to collect the information they need to know and share, Kobus said.

Communication with customers is probably the most important aspect of a company's breach response, according to Kobus. BakerHostetler's report cautions against early over-notification, since

not every incident triggers breach-notification statutes and quickly releasing information that turns out to be unnecessary or inaccurate can cause more harm than good.

Rather, Kobus said, companies should take time to investigate and then provide clear, succinct communications that answer the questions customers are most concerned about — what happened, how did it happen, what are you doing to protect consumers and what are you doing to prevent this going forward. That lowers the chances of being hit with a class action, he said.

"I think a lot of people will get involved in a lawsuit only because they're frustrated," he said. "The company isn't talking to them, isn't helping them do what they need to have done, and that's why a lawsuit will result."

King & Spalding LLP partner Phyllis Sumner, who serves as the firm's chief privacy officer, added that it's important to not treat notices in a cookie-cutter fashion, but to think about the customers and about how regulators would perceive the incident in order to provide notices that convey the right tone and address the incident appropriately.

A notice won't automatically trigger litigation, she said, "but if a notice is sent out in a way that does not comply with the law or in a tone that is inappropriate for the circumstances, or the notice is overbroad and makes it appear as if the incident is much more significant than it is or is inaccurate and downplays the incident — all of those would increase risk rather than decrease risk."

Sometimes, Suits Happen

The number of data breaches that lead to litigation may be relatively small, but lawsuits are sometimes inevitable, experts say.

Oftentimes, the likelihood of litigation is tied to publicity a company may receive as a result of the incident, the profile of the company and the size of the breach, Sumner said.

"We've witnessed that with some of the retail data breaches that received significant coverage and then resulted in a lot of class action activity," she said, pointing to Home Depot and Target as examples.

Bryan Cave's report calls this the "lightning rod" effect, where attorneys file multiple cases against companies tied to the largest, most-publicized breaches and leave the majority of other breach targets alone. The 2016 report found 83 data breach suits filed during the period examined, but only 21 unique defendants.

This is partly because plaintiffs' attorneys know larger companies have deep pockets and more customers, leading to bigger classes and higher potential settlements, experts say. But there's also the simple fact that an attorney has to know about a breach to prosecute it, Bryan Cave associate Joy L. Anderson said.

"If the media is making the information readily available so that you know about the breach, it's natural that … you're going to investigate it and see if there are clients and ways to make it actionable," she said.

The type of information affected can also affect whether suits are filed, Anderson said; there's a huge difference between a compromised email address and a stolen Social Security number.

When sensitive or embarrassing information is compromised — like a 2014 cyberattack at Sony Corp. that made off with several unreleased films and employee data, including medical and salary information — suits are more likely to follow, she said.

"With information that wouldn't otherwise be out there, it's easier to make a case for damages and for people to be more personally affected by a breach, versus just getting a letter in the mail that somebody may or may not have accessed your credit card number," Anderson said. "You get a new credit card, you change your login information, and you sort of move on."

Kobus agreed, saying consumers are becoming numb to some of these breaches and are recognizing

that there will always be incidents, no matter what a company does. It's when consumers see something in a notice that doesn't sit right with them or a practice that should have been ditched a long time ago that they get upset, he said.

At Edelson PC, the attorneys look to whether there is some sort of negligence at the core of a company's behavior when deciding whether to bring a breach class action, Edelson said, explaining that the firm prefers cases where a company clearly dropped the ball.

"In terms of our firm, we don't believe that just because there's a data breach happening that the company necessarily acted improperly or in violation of the law," he said. "If it is an extremely sophisticated attack and the company did everything that it could, then we're going to pass on the lawsuit."

--Editing by Pamela Wilkinson and Kelly Duncan.
