The 6 Lawsuits All GCs Face After A Data Breach

By Melissa Maleske

Law360, Chicago (December 9, 2015, 2:17 PM ET) -- It's not a question of if you'll be hit with a data breach attempt, but when. And if it's successful, the fallout litigation is just as inevitable. Here are the lawsuits you'll field and the parties you'll face after a cyberattack.

Consumers

Consumer class actions are the most ubiquitous of post-breach litigation, but the plaintiffs in these suits still face an uphill climb to establish their standing to sue.

They must show they've suffered concrete actual or imminent injury, not just hypothetical future harm. They also need to be able to trace their injury back to the target of their suit and show that a favorable decision would redress that harm. And that's a high bar to meet, says K Royal, the assistant general counsel and privacy officer at CellTrust Corp.

But it's not impossible. In April, a federal judge had found that consumer plaintiffs had standing to sue Target Corp. following its 2013 credit and debit card data breach. The company quickly settled the case, agreeing to pay up to $10 million to consumers who could document losses they'd suffered. It was a rare win for data breach plaintiffs, but the settlement was also a low dollar amount for a breach that exposed the financial information of up to 70 million consumers.

In July, consumers whose credit card information was stolen in a Neiman Marcus Group Ltd. LLC data breach saw a victory at the Seventh Circuit, which revived claims previously dismissed for lack of standing. The court noted that the plaintiffs "have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information?"

However, other plaintiffs may not be able to connect fraudulent activity in their accounts back to a data breach, as the Neiman Marcus plaintiffs were able to do. And while the Neiman Marcus plaintiffs may end up seeing their day in court, Royal points out that the road to get there has been long.

"This is a wonderfully illustrative case, because it was a 2013 breach that just received the decision in July of this year to proceed, demonstrating how long it can take for these cases to work through the system," Royal says.

In the meantime, Royal says plaintiffs are turning to "some creative alternatives for actual harm,"
including decreased economic value of one’s own data, emotional distress, lost time and inconvenience in offsetting the risk, inability to bargain with a click-through privacy policy contract, and unjust enrichment.

**Financial Institutions**

Another settlement related to the Target breach could change the way card-issuing financial institutions respond to data breaches that expose their customers' information.

On Dec. 2, the retailer announced a $39 million settlement with a class of U.S. financial institutions that had declined to release their claims against Target by entering into separate arrangements with Visa Inc. and MasterCard Inc.

It was the first-ever settlement of a breach-related lawsuit reached on behalf of financial institutions, and it may lead more banks to turn directly to retailers to recoup their losses after a breach, rather than working through post-breach recovery programs established by the payment card companies themselves. In the Target case, the settlement ultimately will yield the banks more money than the Visa and MasterCard programs would have.

Generally these cases have been a tough sell, says Mark Thibodeaux, deputy practice leader of Sutherland Asbill & Brennan LLP’s privacy and cybersecurity team. Meanwhile, the card-issuing banks are usually the parties that bear the brunt of the costs associated with fraudulent charges made using stolen credit card numbers.

"The card-issuing banks usually didn't have any direct relationship to the retailer, so it was difficult for them to sue, and most of the time in the past, they haven't done so," Thibodeaux says. "But I suppose Target involved enough money for them that it made it worthwhile to give it a shot."

However, Thibodeaux doubts the Target settlement will embolden banks to start regularly suing retailers for data breaches that exposed card information, particularly against smaller companies or in cases of smaller breaches.

"In most cases, the harm the banks suffer in the long term is fairly small," Thibodeaux says. "In small cases, the amount of recovery they're going to be able to get from a small retailer is going to be fairly limited and ... the recovery would probably be limited to the limits of the retailer's cyberinsurance policy. I think the banks are still going to do a cost-benefit analysis as to whether they think it's worthwhile in smaller breaches."

**Insurers**

Most companies that handle personal and financial information have seen the writing on the wall and invested in cyberbreach insurance. However, it's not always clear what policies cover or require of the insureds.

For example, does a directors and officers policy cover a breach-related shareholder derivative suit? What kind of security vulnerabilities might trigger an exclusion clause?

"There will certainly be litigation over what cybersecurity insurance really covers," says Claudia Callaway, chair of the consumer finance litigation practice at Katten Muchin Rosenman LLP. "Providers
will say, 'This is where the breach came from, and the policy doesn't cover this exclusion.' Companies need to be savvy when they buy these insurance products."

Sony Corp. of America had duked it out in court with Zurich American Insurance Co. and Mitsui Sumitomo Insurance Co. Ltd. over whether the insurers had to cover the 2011 Sony PlayStation Network breach, in which hackers stole confidential information on tens of millions of users. In 2014, a New York trial judge found that Sony's policy that covered the "publication" of private information could not be triggered by third parties such as hackers. They parties settled in April before an appeals panel ruled on the case, depriving both insurers and the insured of clarity from an appellate court on data breach coverage.

**Shareholders**

Following a breach, companies face massive related costs, including litigation outlays. Some shareholders are starting to go after directors and officers for breaches of fiduciary duty — namely, failing to adequately protect sensitive data in a world where data thefts are commonplace, and mishandling the litigation and enforcement fallout from a breach.

After the Target breach, shareholders filed a derivative suit against 13 officers and directors, alleging breach of fiduciary duty and waste of corporate assets. A similar suit against Wyndham Worldwide Corp. was tossed in 2014. In June, a Home Depot Inc. shareholder sued the company for allegedly failing to secure payment information ahead of a 2014 breach that compromised up to 56 million cards.

As the Wyndham dismissal demonstrates, shareholders also face a high bar. The judge in that case said he found no proof that the Wyndham board's failure to investigate and remedy the hotel's security protocols, as shareholders had proposed, was a sign of bad faith. Wyndham had argued that it reasonably investigated the demand and made a good faith exercise of business judgment in rejecting it.

**Employees**

If breaches expose employee information, companies may face suits from workers.

In 2014, an employee of The Coca-Cola Co. alleged in a putative class action that the company was negligent in failing to secure employee information and failing to promptly notify employees of the theft of 55 laptops containing employees' personally identifiable information. In October, a judge threw out many of his claims, but allowed breach of contract and unjust enrichment claims to stand.

While Coca-Cola's breach stemmed from a traditional theft, Katten senior counsel Christina Grigorian says, those claims are quite cutting-edge. In particular, the unjust enrichment claims are "a really novel theory predicated in a company's failure to provide adequate resources to the protection of personal nonpublic information," she says.

**The Government**

Both federal and state enforcement authorities may come knocking after a breach, depending on the nature of the breach, the information it compromised and the readiness and response of the company in question.

If health information is compromised, the U.S. Department of Health and Human Services will surely
take a look at the situation and bring an enforcement action if a company is found to have violated the Health Insurance Portability and Accountability Act. In 2013, for example, WellPoint Inc. had to shell out $1.7 million to settle alleged HIPAA violations related to a 2009-2010 breach of the managed care company.

The Federal Trade Commission also can sue companies for failing to live up to their stated security standards, a deceptive trade practice, or not providing adequate security — an unfair trade practice. The Third Circuit recently gave its blessing to the unfairness approach in an FTC action against Wyndham.

The HHS and FTC are merely the tip of the iceberg, and different industries will have to face their relevant government agencies. The Consumer Financial Protection Bureau can bring enforcement actions for unfair, deceptive or abusive conduct, which may cover security lapses. Government contractors will face scrutiny from the U.S. Department of Defense, which recently issued cyber-reporting rules. The FCC recently brought its third cybersecurity enforcement action against Cox Communications Inc.

And the U.S. Securities and Exchange Commission has been increasingly interested in cybersecurity. In September, the commission fined R.T. Jones Capital Equities Management Inc. for allegedly failing to adhere to a safeguards rule in the securities laws. The SEC said the investment adviser did not adopt written policies and procedures ahead of its breach that compromised the information of 100,000 individuals.

Then there are the state attorneys general. Forty-seven states now have breach notification laws, and states including California — the first to adopt a notification statute — and Connecticut are creating and strengthening laws to empower them to pursue companies that fail to properly protect sensitive information.

Callaway says companies can avoid entanglements with law enforcement by adopting and adhering to solid security protocols. And immediately after a data breach, they should determine their reporting requirements and comply with them.

It's "a perilous course" if a company or its employees tries to cover up a data breach, Callaway says: "That's where a company can draw the attention of federal regulators."

--Additional reporting by Jody Godoy, Allison Grande, Jeff Sistrunk and Steven Trader. Editing by Katherine Rautenberg and Edrienne Su.