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

Equifax Data Breach Highlights Regulatory Shortfall

By **Evan Weinberger**

Law360, New York (September 8, 2017, 8:45 PM EDT) -- Equifax's Thursday announcement that a security breach put the names, Social Security numbers, addresses and other personal data belonging to roughly 143 million consumers at risk highlighted gaps in U.S. regulations for the consumer credit reporting industry.

While the Consumer Financial Protection Bureau has authority to police violations of consumer protection laws by consumer credit bureaus and the Federal Trade Commission plays a role as well, responsibility over monitoring cybersecurity protections at such firms remains unclear, experts say.

And the company's heavily criticized public response to the breach has raised questions about whether a federal standard for reporting a hack and how to protect potentially affected consumers is necessary.

"This is now one of a series of high-profile cyber events that have occurred over the last several years in which outside entities have been able to gain access to systems and extract sensitive information and, in some instances, use it for illegal purposes," said John Cohen, a former acting undersecretary for intelligence and analysis at the U.S. Department of Homeland Security.

"It begs the question: Why is there not a more unified effort by the federal government to work with the private sector?" said Cohen, now a professor at Rutgers University.

Equifax Inc. revealed Thursday after the stock market closed that hackers had exploited a flaw in its website allowing them to get access to account information for up to 143 million customers. While it is unclear exactly how much information had been stolen, what is clear is that the hackers made off with information that makes the Equifax breach more damaging than some of the other high-profile and numerically larger hacks of recent years.

In particular, the Social Security numbers that hackers were able to gather would allow them to impersonate a consumer in just about any electronic transaction since that identification number is typically used to verify an account applicant's identity.

"They've got so much critical information," said Steven Moore, a partner at Withers Bergman LLP.

The sheer scale of the breach, as well as confusion over whether Equifax would attempt to force consumers into arbitration over it, resulted in a flurry of responses from lawmakers and law enforcement officials around the country.

New York Attorney General Eric Schneiderman as well as attorneys general from Massachusetts, Pennsylvania and other states announced investigations into the breach, which is also being investigated by the FBI.

The CFPB is also conducting an investigation, bureau spokesman Sam Gilford said in a statement.

"The CFPB is authorized to take enforcement action against institutions engaged in unfair, deceptive or abusive acts or practices, or that otherwise violate federal consumer financial laws. We are looking into the data breach and Equifax's response, but cannot comment further at this time," he said.

Democrats, including Sens. Sherrod Brown of Ohio, Elizabeth Warren of Massachusetts and Mark Warner of Virginia and Rep. Maxine Waters of California blasted Atlanta-based Equifax for imposing an arbitration clause on the credit monitoring service that it was providing for affected individuals.

"It's shameful that Equifax would take advantage of victims by forcing people to sign over their rights in order to get credit monitoring services they wouldn't even need if Equifax hadn't put them at risk in the first place," Brown said in a statement.

Even Republican lawmakers got into the act, with House Financial Services Chairman Jeb Hensarling of Texas announcing that his committee would hold a hearing on the breach, although he did not set a date.

"This is obviously a very serious and very troubling situation and our committee has already begun preparations for a hearing," Hensarling said in a statement.

Consumer advocates and cybersecurity experts pointed to a few areas where government could improve the landscape for guarding key financial data held by consumer credit bureaus.

First, consumer advocates urged the Senate to reject a bid to nullify a recent CFPB rule eliminating the use of class action bans in arbitration clauses, which would allow the kinds of lawsuits that have already been filed against Equifax to proceed without fear that they would be sent to arbitration.

A resolution under the Congressional Review Act to overturn the rule has already passed in the U.S. House of Representatives, but its fate remains unclear in the Senate as of now. Some estimates have Republicans between three and five votes short of getting the support necessary to nullify the rule.

"Repealing crucial consumer protections as new financial scandals break every week would send a clear signal to bad actors like Equifax and Wells Fargo that they can continue to plunder consumers for profit," said Amanda Werner of Public Citizen and Americans for Financial Reform.

Beyond arbitration, advocates said that the government should look to set up some sort of federal standard both for monitoring the protocols in place to protect against a breach and on how to handle it.

On the supervisory front, there are questions about which federal regulators could step in to monitor consumer credit bureaus for cybersecurity preparedness. While the CFPB has the power to supervise the largest players in the market, including the big three of Equifax, Experian and TransUnion, for adherence to the Fair Credit Reporting Act, it's unclear whether they have the authority to do regular supervision on cybersecurity.

The CFPB hit Dwolla Inc. with an enforcement action in March 2016 for cybersecurity violations under its expansive powers to pursue potential claims of unfair, deceptive and abusive acts and practices, specifically citing the firm's claims about the quality of its security measures and encryption of sensitive information.

The CFPB's Gilford did not comment on that issue.

Cohen said that having a central authority to provide cybersecurity guidelines and supervision similar to what the federal and state banking regulators provide to banks could be helpful so that all firms are up to speed.

Currently, Homeland Security and other government entities provide information sharing and best practices, but more could be done, he said.

That idea is likely to generate pushback from industry, and with a Trump administration in place that has said it wants to roll back regulations, implementing such a plan is likely far off, Cohen said.

"I think the likelihood of any types of mandates right now, even in an area like cybersecurity, is minimal," he said.

On the consumer side, activists say that federal standards for when a breach is reported and for applying free credit freezes could help people who were subject to their data getting out into the open.

Equifax knew about the breach in July but did not report it until September, and state laws regarding credit freezes vary. In most, consumers have to pay.

Although Republicans may be willing to hold hearings on Equifax, they are also supporting House bills that could ease the regulatory environment of such firms. The House Financial Services Committee held a hearing on some of those bills just hours before Equifax's announcement.

"We hope that all members of Congress can stand up for the rights of those 143 million people, as opposed to entertaining the interest of Equifax and the credit reporting companies," said Christine Hines of the National Association of Consumer Advocates.

Representatives for Rep. Barry Loudermilk, R-Ga., the sponsor of one of those bills, said the congressman could not comment due to preparations for Hurricane Irma's landfall.

However, even with enhanced supervision of cybersecurity and increased consumer protections, credit bureaus are going to remain targets and they are going to suffer breaches, so increasing encryption of sensitive data and other measures will be vital.

"When you have a persistent threat that's well-resourced, it's a tough battle to win in the long term," said Marcus Christian, a Mayer Brown LLP partner and former federal prosecutor.

--Editing by Katherine Rautenberg and Catherine Sum.
