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 Fallout Could Boost Consumers' Shaky Harm Claims

By **Allison Grande**

Law360, New York (October 6, 2017, 11:29 PM EDT) -- Legislators in grilling Equifax over its massive data breach proposed fining businesses for each piece of data compromised by hackers, signaling a potentially new approach to lawmaking that could make it easier for consumers to recover damages they struggle to get in litigation.

Members from both sides of the aisle, including Rep. Joe Barton, R-Texas, and Sen. Elizabeth Warren, D-Mass., floated the consumer-oriented moves during Senate and House Committee hearings with Equifax's former CEO Richard Smith over the breach, which was first disclosed on Sept. 7 and led to the exposure of Social Security numbers and other private data belonging to 145.5 million Americans.

The hearings offered businesses a crash course in the tricky tightrope they have to walk when it comes to post-breach disclosures and the importance of having a tested breach response plan in place. They also highlighted the fact that lawmakers are starting to push for fixes that would not just improve security but help consumers as well, even if those proposals don't necessarily boost cybersecurity in the long run, attorneys say.

"To my mind, the most remarkable thing to come out of the congressional committee hearings of Equifax's Richard Smith are the comments from both Joe Barton and Elizabeth Warren that there should be modification for data breach laws to compensate the consumers who are victims of the attacks," said Timothy Toohey, the head of Greenberg Glusker Fields Claman & Machtinger LLP's cybersecurity practice. "If such laws were passed, this would be a remarkable change in the paradigm for data breach notification laws."

The breach reporting statutes currently on the books in 48 states, along with a handful of state data security laws and federal laws that protect narrow sets of data such as health and financial information, have primarily been "informational in nature and have placed the onus on the consumer to monitor his or her credit, sometimes with the assist of credit monitoring provided by the entity that was breached," Toohey noted.

But under the suggestions put forth by Barton, Warren and others, which would essentially establish fixed statutory damages for consumers, the burden would shift to companies to ensure that consumers are made whole, regardless of whether individuals have suffered identity theft or any other actual harm, according to Toohey.

“This would be a major change from current laws because it would potentially lead to significant financial consequences when a large number of consumers have suffered a breach,” he said. “It would also be a major departure from the burdens that consumers have faced in civil litigation in showing that they have suffered actual damages from a breach.”

Arguments that consumers cannot move forward with negligence and related claims in the wake of data breaches because they lack sufficient injury to establish Article III standing have hobbled putative class actions against several entities, ranging from Michaels Stores to the U.S. Office of Personnel Management.

But the overarching sentiment of the hearings, that consumers need not only answers but also more concrete protections post-breach, indicates that there is at least a willingness to ease these obstacles to recovery, attorneys say.

“Although consumers often believe that they have been harmed when personal data is exposed in a breach, companies are often able to avoid liability — particularly in civil lawsuits — because there is no demonstrable financial harm,” Toohey said. “Legislators seem to be recognizing that regardless of whether a consumer has suffered financial losses ... they have been harmed by having information exposed and through the fear or concern regarding potential harm.”

In floating the idea at a House Energy and Commerce Committee hearing Oct. 3, Barton argued that requiring companies to provide compensation to affected individuals could make them “pay a little more attention to data security.”

"I think it's time at the federal level to put some teeth into this and require some sort of per account payment,” the lawmaker said. “I don't want to drive credit bureaus out of business and all of that, but we could have this hearing every year from now on if we don't do something to change the current system."

While imposing fines would certainly get businesses’ attention, several attorneys were skeptical that the penalty alone would cause companies to invest more in data security.

Equifax has reported spending $250 million on security measures in the three years leading up to the breach, and will likely have to spend millions if not billions more in providing consumers with remediation services and otherwise recovering from the incident, attorneys noted.

“If companies were told in advance that if they have a breach they would be fined $1,000 per record, I don’t think that would create an incentive that keeps that breach from occurring,” said Nathan Taylor, a partner with Morrison & Foerster LLP’s privacy and data security and banking and financial services practices. “That type of legislation is more about punishment and appeasing consumers than it is about necessarily improving security.”

Taylor pointed out that Fortune 500 companies are already taking note of the hefty price tag Equifax and other targets that have come before it have had to foot in the wake of breaches, and are well aware that cleaning up a breach will cost them significantly even without additional fines.

“That creates a pretty strong incentive on its own,” he added.

The move to fine companies could also cause those that have been breached to be less forthcoming

about what happened and more conservative in estimating how much information hackers may have actually gotten their hands on, as opposed to just may have had access to, attorneys noted.

“What’s important in trying to craft legislation in this context is balancing punishing those companies and creating incentives for them to report what happened,” said Glen Kopp, a Bracewell LLP partner and former prosecutor in the Southern District of New York. “It’s one thing to tell companies that they must report a breach, but when you’re threatening companies with fines and sanctions per individual whose information has been stolen, you start incentivizing people to limit how much they find out or disclose about the scope of the breach.”

Congress passed legislation in late 2015 to encourage the public and private sectors to exchange more data more quickly about what threats they’re seeing and how hackers are getting into their systems, and a resulting early disclosure of threat indicators could help other companies to avoid making similar missteps, attorneys noted.

In Equifax’s case, an employee had failed to notify the security team of a patch they were supposed to install on the consumer dispute portal, and the scanning system failed to detect that vulnerability.

“You really have to be careful because you want people to know what happened to companies that have suffered breaches and want them to acknowledge what happened to them,” Kopp said. “It’s not a radical or crazy idea to fine companies, but there is a downside to it that should be seriously considered.”

Evan Wolff, a Crowell & Moring LLP partner, said that while a proposal like Barton's may be an "element of what needs to be done," a more holistic examination of the drivers and causes of data breaches by both the private and public sectors will likely be needed, similar to measures taken in the late 1960s and early 1970s to address environmental protection and pollution issues.

"We need to have better guidelines either from government or through public-private initiatives on what is expected from companies in terms of securing and protecting data, because it's still largely unclear what is required of them," Wolff said.

The congressional hearings also brought to light other proposals aimed at ensuring such a massive breach does not happen again, including replacing Social Security numbers as the touchstone for identity verification in the U.S. as well as longstanding suggestions to create federal breach reporting and data security standards.

The Social Security number proposal, which has won backing from both Equifax's ex-CEO and White House Cybersecurity Coordinator Rob Joyce, drew similar criticisms from attorneys, who found that while it wouldn't hurt, it ultimately strays from a holistic approach to securing systems that is necessary to tackle complex and steadily increasing cyberthreats.

"While this is a conversation we should absolutely have, the discussion is fundamentally premised on disincentivizing threat actors by impacting their demand, so if you replace the Social Security with XYZ number, what we'll see is threat actor demand would shift from Socials to XYZ," Taylor said. "We don't have a Social Security number issue, we have a cyber threat and resilience issue, and the biggest challenge of this generation is how do we secure ourselves in this automated and internet-connected world."

Proposals to set common breach reporting and security standards, such as legislation that was re-introduced Oct. 2 by Rep. Jan Schakowsky, D-Ill., come closer to addressing cybersecurity in a way that could help reduce breaches, attorneys say.

But lawmakers have pushed for these kinds of protections after practically every major breach since Target announced the compromise of more than 40 million payment cards during the 2013 holiday season, and efforts have been hampered by disputes over whether the measures should fully preempt state laws and whether attorneys general and consumers should be given the right to sue companies over failing to timely report breaches or properly institute certain security standards.

"After the Equifax breach, we're probably a step closer to seeing this kind of legislation enacted, but it's unclear if we're there yet," Taylor said.

However, regardless of whether Congress pushes through any of these recent proposals, attorneys noted that there's really no "silver bullet" legislation that will wipe away the threat posed by sophisticated nation states and other motivated hackers.

Rep. Greg Walden, R-Ore., said as much in the House Commerce Committee on Oct. 3, when in response to Smith's repeated insistence that the Equifax breach could be attributed to a combination of human error and technology failure, he remarked he didn't think his colleagues could pass a law that "fixes stupid."

"Congress could pass a law that is designed to limit the risk of human error, such as having requirements that personnel have appropriate skill sets and training, but they can't legislate in a way that prevents human error," Taylor said. "Whether we need a federal law to elevate the level of corporate data security in this country, that may be true. But while federal legislation may prevent some of these incidents, it won't prevent all of the very serious ones, and we'll likely always keep coming back to the drawing board."

--Editing by Pamela Wilkinson and Breda Lund.