Communications Daily

House Committees' Coming Equifax Data Breach Hearings May Not Change Things Much, Experts Say

Communications Daily

12 September 2017

Two House committees plan hearings on the Equifax data breach to see how future attacks can be prevented and information better protected. Such efforts may not amount to much, some experts told us. They said the onus falls on consumers to proactively ensure their data is protected.

"I am deeply concerned about the cyberattack against Equifax that may have affected 143 million American consumers and that it took the company over a month to notify the public," said House Judiciary Committee Chairman Bob Goodlatte, R-Va., in a statement. He said his committee plans a hearing on the breach and on whether current laws can be improved to prevent attacks and bolster privacy. Rep. Ted Lieu, D-Calif., urged Goodlatte and ranking member John Conyers, R-Mich., in a Friday letter to hold the hearing on the attack and invite representatives from Experian and TransUnion to find out what they're doing to prevent breaches. Lieu, a committee member, said Congress has a "strong" role to play in preventing attacks and hold accountable those holding such sensitive data.

Chairman Greg Walden, R-Ore., said the House Commerce Committee will hold a hearing on the breach to see how lawmakers can better protect consumers from breaches, and FTC Commissioner Terrell McSweeny and Sen. Mark Warner, D-Va., sought regulatory action such as a national data breach notification law (see 1709080019). Financial Services Committee ranking member Rep. Maxine Waters, D-Calif., said last week she plans to reintroduce legislation that would mitigate ID theft. Attorneys general of New York Eric Schneiderman and Illinois' Lisa Madigan announced investigations.

In assessing the breach, AT&T said its systems and data weren't targeted. "However, we understand that the impacts include current and former consumer and business customers of AT&T," it said in a Saturday news release, saying those customers should find out if they've been affected and sign up for credit file monitoring and ID theft protection.

Neal O'Farrell, executive director of the Identity Theft Council, said the value of the breached Equifaxrecords, including names, addresses, birth dates, and driver's license and Social Security numbers, is very high, and could spur action to do something about large data breaches. But he said: "I'm absolutely certain that Equifax's strategy is to hold its breach, take the licks and, in a couple of weeks, we'll have moved on because every other data breach has followed exactly

the same pattern." O'Farrell said he's most worried about the incident's impact on consumer confidence.

Paige Schaffer, president of Generali Global Assistance's identity and cyber protection services global unit, said more regulatory action may come. "This government tends to be pro-business, not so much consumer, and certainly supportive of big data," she said. One possibility might be tightening the data breach notification law in Georgia where Equifax is based. She said the credit reporting service took longer than it should have to notify consumers about the breach. She said the "hyper nervousness" about the incident may drive more consumer awareness, resulting in people being unwilling to share their data unless they feel protected.

Consumers complained they would have to waive their rights to a class-action lawsuit and submit to arbitration if they accepted Equifax's credit protection product, Sen. Elizabeth Warren, D-Mass., tweeted last week. The credit reporting bureau said Monday the arbitration clause and class-action waiver in the terms of use didn't apply to the breach.

Schaffer said she talked with executives at TransUnion, which wasn't breached, who are taking the incident seriously and are looking to ensure data protection within their organization. O'Farrell said Congress, law enforcement and consumers have roles to play but so much personal data already has been breached that criminals are having a hard time keeping up. Both experts said consumers have the bigger burden to protect their data through reviewing bank statements and credit reports or subscribing to credit monitoring, credit freeze and fraud alert services. Credit freezes, noted O'Farrell, could make consumer information "economically unviable" for hackers to exploit. But consumers, who've been "apathetic" for years on the issue, "have to start getting pissed," he added.