Equifax breach: Criticism from lawmakers, what people can do

8 September 2017, by Ken Sweet

This July 21, 2012, photo shows Equifax Inc., offices in Atlanta. Credit monitoring company Equifax says a breach exposed social security numbers and other data from about 143 million Americans. The Atlanta-based company said Thursday, Sept. 7, 2017, that "criminals" exploited a U.S. website application to access files between mid-May and July of this year. (AP Photo/Mike Stewart)

There's no way around it: The news from credit reporting company Equifax that 143 million Americans had their information exposed is extremely serious.

Crucial pieces of personal data that criminals could use to commit identity theft—Social Security numbers, birthdates, address histories, legal names—were all obtained. That's information that cannot change. And once that data is out there, it's basically out there forever.

"The crown jewels of personal information were exposed and potentially stolen," said John Ulzheimer, an independent credit consultant who previously worked at Equifax.

Equifax's key role in the financial industry makes this breach more alarming than previous ones at Yahoo or retailers. It's a storehouse of personal information, like how much people owe on their houses and whether they have court judgments against them.

Lenders rely on the information collected by three big credit bureaus—Equifax, TransUnion and Experian—to help them decide whether to approve financing for homes, cars and credit cards. Credit checks are sometimes done by employers when deciding whom to hire for a job.

Atlanta-based Equifax said Thursday that "criminals" exploited a U.S. website application to access the files between mid-May and July of this year. It discovered the hack July 29, but waited until Thursday to warn consumers.

AS A CONSUMER, WHAT TO DO:

Beyond the usual steps of checking credit reports regularly and watching for abnormal transactions on your accounts, it may be time to take more extreme measures to lock down your information.

The strongest possible option a person can take immediately is placing what's known as a credit freeze on their files with the major credit bureaus. That locks down a person's information, making it impossible to open new accounts and bank cards in their name.

But taking that option also locks you out from opening new accounts. It also can come with a fee with each of the bureaus, depending on which state you live in.

"The credit freeze is the nuclear option of credit protection. But in the wake of a breach this big, it's worth considering," said Matt Schulz, an analyst with CreditCards.com.

Consumers will need to be more careful about

checking their credit reports. U.S. law gives every American the right to get those files for free once a year from the three major bureaus. While many websites market access to your credit reports, the official one is annualcreditreport.com.

It's best to spread those requests out over the year—do one every four months, experts say. And expect to check this information not just in the immediate future, but for the long term—potentially years.

"Bad guys can be very patient with data. This should be a wake-up call to be even more diligent with your information," Schulz said.

Ulzheimer says an option consumers should consider is setting up fraud alerts on your files. That would require creditors to contact you directly, usually by phone, for approval before allowing an account to be opened. That gives people a more active role, rather passively monitoring or freezing your entire file. Bureaus also must contact each other when a fraud alert is placed.

Need an even more extreme step? People can request to change their Social Security number with the Social Security Administration if they have repeatedly been a victim of identity fraud under their original number.

Equifax has a website, www.equifaxsecurity2017.com/, where people can check if their information may have been stolen. Consumers can also call 866-447-7559 for information. The company also says it will send mail to all who had personally identifiable information stolen.

SIZE AND SCOPE

This isn't the biggest data breach in history. That indignity still belongs to Yahoo, which was targeted in at least two separate digital burglaries that affected more than 1 billion of its users' accounts throughout the world. But no Social Security numbers or drivers' license information were disclosed in the Yahoo break-in.

Equifax's security lapse could be the largest theft involving Social Security numbers, one of the most common methods used to confirm a person's identity in the U.S. It eclipses a 2015 hack at health insurer Anthem Inc. that involved the Social Security numbers of about 80 million people.

Any data breach threatens to tarnish a company's reputation, but it is especially mortifying for Equifax, whose entire business revolves around being a secure storehouse and providing a clear financial profile of consumers that lenders and other businesses can trust.

And a security expert said the website created Equifax to help customers find out if their information was stolen raises its own security questions. The site looks like the kind set up by attackers to trick people into disclosing information, says Georgia Weidman, founder and chief technology officer for security firm Shevirah.

"It's teaching people entirely the wrong things about using the internet securely," Weidman said. She said says she's also troubled by Equifax's approach to security generally, including reports that it didn't respond to basic scripting bugs it was warned about last year.

In addition to the personal information, Equifax said the credit card numbers for about 209,000 U.S. consumers were also taken, as were "certain dispute documents" containing personal information for approximately 182,000 people in the U.S.

The company said hackers may have some "limited personal information" about British and Canadian residents, but doesn't believe that consumers from other countries were affected.

FALLOUT

The enormity of the breach has put immense financial and political pressure on Equifax.

Washington regulators and politicians swiftly criticized Equifax, and Jeb Hensarling, chairman of the House Financial Services Committee, said he will call for Congressional hearings.

Equifax's requirement that affected customers sign

up for arbitration also drew a backlash. Democrats in the House and Senate called on the company to pull back its requirement that anyone who signs up for credit monitoring give up their right to sue Equifax in a class-action lawsuit.

The Consumer Financial Protection Bureau, the nation's chief watchdog for financial services, called the breach "troubling" and said Equifax should drop the arbitration requirement. The CFPB recently passed a rule requiring financial companies to let customers sue together when a large group has been wronged.

Several state attorneys general also stepped in. New York's attorney general, Eric Schneiderman, said he was starting his own investigation.

Company executives are also under scrutiny, after it was found that three Equifax executives sold shares worth a combined $1.8 million just a few days after the company discovered the breach, according to documents filed with securities regulators. Equifax said the three executives "had no knowledge that an intrusion had occurred at the time they sold their shares."

Equifax shares fell about 13 percent to $123.75 in heavy trading. The decline equates to about $2.28 billion in lost market value.