Equifax breach sows chaos among 143M Americans

September 9 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)

A day after credit-reporting company Equifax disclosed that "criminals" had stolen vital data about 143 million Americans, it had somehow

managed to leave much of the public in the dark about their exposure, how they should protect themselves and what Equifax planned to do for those affected.

The breach is unquestionably serious. It exposed crucial pieces of personal data that criminals could use to commit identity theft, from Social Security numbers and birthdates to address histories and legal names.

That data—the "crown jewels of personal information," in the words of independent credit analysts John Ulzheimer—can't be changed, and once it's in circulation, it's basically out there forever.

But Equifax's response has satisfied almost no one.

UNHAPPINESS EVERYWHERE

Consumers complained of jammed phone lines and uninformed representatives. An Equifax website set up to help people determine their exposure looked like a scam to some, and provided inconsistent and unhelpful information to others. Congress planned hearings.

Anders Ohlsson, a 47-year-old technical manager in Scotts Valley, California, called a hotline multiple times and was disconnected; entered the last six digits of his Social Security number into Equifax's emergency website; and finally spoke with a call center manager. He still doesn't know whether his information has been compromised.

"I don't think I've gotten hold of a person that actually cares," he said. "Now they're fumbling to tell people what's going on. But they really don't know what's going on."

Equifax plays a key role in the financial industry, making 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 on financing for homes, cars and credit cards. Credit checks are sometimes done by employers when deciding whom to hire for a job.

WHAT YOU CAN DO

Even if you don't know if you're one of the 143 million, you might want to consider extreme protective measures.

Your strongest immediate option involves placing a credit freeze on their files with the major credit bureaus. That locks down your information, making it impossible for outsiders to open new accounts and bank cards in your name. But it also blocks you from opening new accounts, and might involve fees depending on the state you live in.

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

You should also be more diligent about checking your credit reports, where you can see if anyone has opened unauthorized accounts in your name . You can get those files for free once a year from the three major bureaus; use the official site, annualcreditreport.com .

It's best to spread those requests out by getting one every four months. And you'll need to be ready to keep checking for a while—potentially years.

"Bad guys can be very patient with data," Schulz said.

If you're not ready for the freeze, Ulzheimer recommends setting up fraud alerts on your files. These force creditors to contact you directly, usually by phone, for approval before approving an account.

And if you've been a victim of repeated identity fraud, you can request a new Social Security number with the Social Security Administration.

In addition to the emergency Equifax website, www.equifaxsecurity2017.com/, you can also call 866-447-7559 for information. The company also says it will send mail to all who had personally identifiable information stolen.

HOW EQUIFAX REACTED

Any data breach threatens to tarnish a company's reputation, but Equifax hasn't done much to minimize that damage.

Atlanta-based Equifax said Thursday the breach took place between mid-May and July of this year. It discovered the hack July 29, but waited until Thursday to warn consumers.

Or take the company's emergency-information website. To Georgia Weidman, founder and chief technology officer for security firm Shevirah, it looks a lot like the kind of site scammers would use to trick people into giving up passwords or other crucial information.

"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.

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—one of them the company's chief financial officer—didn't know about the breach at the time of the sales.

Equifax's security lapse could be the largest theft involving Social Security numbers, one of the most common ways 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 .

FALLOUT

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.

New York's attorney general, Eric Schneiderman, said he was starting his own investigation.

In a statement Friday evening, Equifax said it had fixed problems with

the emergency website and tripled its call center team to over 2,000 agents. It also declared that the arbitration requirement and class-action waiver will not apply to this particular breach.

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