What you need to know about the Equifax data breach

9 September 2017, by The Associated Press

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)

Equifax, one of the three main credit reporting companies, said this week that a major data breach exposed Social Security numbers and other important information of millions of people.

The breach affected about 143 million in the United States, as well as some people in Canada and the United Kingdom, but Equifax didn't provide a number. Hackers had access to the data between May and July, Equifax said. The company discovered the hack on July 29 and publicly announced it more than a month later on Thursday.

Here's what else you need to know about the breach:

___

WHAT INFORMATION WAS TAKEN?

Hackers had access to Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers and other information. Those are all crucial pieces of personal data that criminals could use to commit identity theft. Those are what John Ulzheimer, an independent credit consultant who previously worked at Equifax, called "the crown jewels of personal information."

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. The data breach is especially damaging to Equifax, since its entire business revolves around being a secure storehouse and providing a clear financial profile of consumers that lenders and other businesses can trust. The credit profiles it holds contain personal information, like how much people owe on their houses and whether they have court judgments against them.

___

AM I AFFECTED?

Equifax set up a site, equifaxsecurity2017.com , where you can type in your last name and six digits of your Social Security number to find out if your data may have been compromised. Consumers can also call 866-447-7559 for information. The company says it will send mail to all who had personally identifiable information stolen.

Equifax is also offering free credit monitoring for a year. The company says the service will search suspicious sites for your Social Security number, give you access to your Equifax report and other offerings. You can sign up at the same site listed above, and the deadline to do so is Nov. 21.

Initially, though, there was a catch—signing up would also commit you to binding arbitration with

the credit monitor, which would mean giving up your right to sue. Several politicians and consumer groups have criticized this provision. Democrats in the House and Senate called on the company to pull back that requirement. Late Friday, Equifax said the arbitration language that appears on its website "will not apply to this cybersecurity incident."

___

WHAT SHOULD I DO?

You can view your credit reports for free at AnnualCreditReport.com. You're entitled to get a free copy of your credit report from each of the three big agencies once every 12 months. Review it closely for unauthorized accounts or any mistakes.

And you may need to be vigilant much longer than the free year of credit monitoring Equifax is offering. "If any of the data was exposed, you will be living with that for the rest of your life," said Rich Mogull, who runs the security research firm Securosis.

You can consider freezing your credit reports, but it comes with some downsides. A freeze stops thieves from opening new credit cards or loans in your name, but it also prevents you from opening new accounts. So each time you apply for a credit card, mortgage or loan, you need to lift the freeze a few days beforehand.

Freezes can be done online at the websites of the three credit reporting agencies—Equifax , Experian and TransUnion . You'll need to freeze all three reports for the best protection. Each company will give you a code that you'll need again in order to lift the freeze, so keep it in a safe place. When you plan to apply for a credit card, mortgage, or other loan you'll need to go back to each site and lift the freeze.

The credit reporting agencies may charge a fee, usually under $10, depending on which state you live in. But it's free for residents of some states, including Maine, New Jersey and South Carolina.

A freeze doesn't protect you from everything: thieves can still file a fraudulent tax return in your name or charge things to your already opened credit card accounts. A freeze won't affect your credit score or report. The report stays open and is updated to keep track of your debts, payments and other information.

___

HOW DID THIS HAPPEN?

Equifax is blaming an unspecified "website application vulnerability." Security experts say it's hard to say for sure without more information, but such vulnerabilities typically don't require a lot of sophistication to exploit.

Mogull says the web app breach suggests "things are broken down in a couple of different areas." He says someone likely made a programming or configuration mistake.

Corporate culture could also be a factor. Often, Mogull says, corporate security is underfunded or isn't given the authority it needs to make sure application developers do what's right.

Ryan Kalember of the security company Proofpoint says that even if the vulnerability was known and fixable, "coordination between app developers and security teams in a lot of organizations are not on the best of terms."

Another security expert said the website Equifax created to help customers find out if they were affected 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.

___

WHO'S INVESTIGATING THIS?

Potentially, a lot of people. Credit bureaus like Equifax are lightly regulated compared to other parts of the financial system.

U.S. Rep. Jeb Hensarling, chairman of the House Financial Services Committee, said he will call for Congressional hearings. And Rep. Greg Walden, the chairman of the House Energy and Commerce Committee, says he'll hold a hearing examining what wrong and how to better protect against future hackings.

Several state attorneys general have also said they would investigate, including those from New York, Massachusetts and Pennsylvania. New York's attorney general, Eric Schneiderman, said his office aims to "get to the bottom" of how the breach occurred.

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."