

Equifax data breach: What you need to know about hacking crisis

[Nathan Bomey](#), [Alia E. Dastagir](#), [Adam Shell](#), [Kevin McCoy](#) and [Roger Yu](#), USA TODAY

Published 2:47 p.m. ET Sept. 15, 2017 | Updated 12:19 p.m. ET Sept. 18, 2017

The [Equifax hacking](#) has created uncertainty over an estimated 143 million Americans who could be facing a serious threat of identity theft for the rest of their lives, spawned government investigations and a triggered a national rush among consumers to protect themselves.

Here's what you need to know about what experts say is potentially the most threatening financial data breach in American history.

How could this happen?

Equifax [failed to promptly install a security fix](#) to a flaw found in a web application tool used by many major corporations, experts said.

Hackers took advantage of that window, which lasted at least two months, to penetrate the company's digital defenses. That allowed them to gain access to the personal data of up to 143 million people.

What did they take?

The hackers seized names, Social Security numbers, birth dates, addresses and even some driver's license information.

"It's very problematic for hackers to have all that important information all in one place," said John Ulzheimer, a credit expert who once worked for Equifax and credit-score firm FICO.

"This information is perpetually valuable. You are not going to change your name or date of birth or Social Security number. In five years they will be the same, unlike a credit card that takes five minutes to cancel over the phone."

How do I know if I was affected?

Visit [Equifaxsecurity2017.com](#) and enter your information to see if Equifax believes your data may have been exposed. Either way, the company is offering free identity-theft insurance, third-party credit-file monitoring, a credit report and other services.

You'll have to officially sign up for those services after checking to see if you might be affected. If you sign up for this service you would not be relinquishing your right to sue Equifax or be compensated through any potential settlement over the cyberbreach.

Equifax is still trying to determine how many people were actually affected.

What are the risks of this hack to me?

If you don't take action to protect yourself, hackers could eventually sell your data to other criminals who could then use it to take out loans in your name, get credit cards, perpetuate tax fraud, access your medical benefits and countless other illegal activities.

How can you protect yourself?

Experts say [freezing your credit is one line of defense](#). That way, if criminals try to use your personal data to take out a loan, credit or services in your name, they'll be blocked from doing so.

"When a financial institution goes to pull your credit report, they simply won't be able to get it," CFRA Research analyst Keith Snyder said. If that happens a person using your information to say, open up a credit card, will probably get turned down.

Other important steps: Monitor your bank records, credit card charges and other bills carefully — ideally once a week. If you spot anything strange, contact the respective company immediately to flag the irregularity.

"You never know for sure 100%, but you should assume your data has been compromised either in this breach or in previous breaches," Gartner security analyst Avivah Litan said.

How do I freeze my credit?

Contact all four agencies directly, said Avivah Litan, a security analyst at financial research firm Gartner:

Equifax: Call 1-800-349-9960 or visit [Freeze.equifax.com/](https://www.equifax.com/freeze).

Experian: Call 1-888-397-3742 or visit [Experian.com/news/security-freeze.html](https://www.experian.com/news/security-freeze.html).

TransUnion — Call 1-888-909-8872 or visit [Transunion.com/credit-freeze/place-credit-freeze](https://www.transunion.com/credit-freeze/place-credit-freeze).

Innovis — Call 1-800-540-2505 or visit [Innovis.com/personal/securityFreeze](https://www.innovis.com/personal/securityFreeze).

Fees vary by state and range from about \$5 to \$10. Equifax has temporarily waived its fees for this service. You'll need to provide personal information, including your Social Security number, to authenticate your identity.

What if I need to unfreeze my credit?

When you freeze your credit you'll get a special personal identification number to use to thaw your credit when you want to take out a loan. Keep the PIN safe and think twice before putting it on an Internet-connected device.

If you need to do anything that will require credit, you'll have to think ahead and unfreeze your credit beforehand, which takes up to three business days.

What are some other ways to monitor my credit?

People are typically advised to access a free copy of their credit report from the major credit reporting companies annually. Given the scope of this hack, some people may want more help. [There are a number of services that you can pay for to monitor credit including MyFico and LifeLock.](#)

Is Equifax being investigated?

Yes. The FTC, Consumer Financial Protection Bureau and multiple U.S. senators [have launched probes into the scandal.](#)

Sen. Elizabeth Warren (D-Mass.) [called Friday for a more thorough government investigation](#) asked Equifax's competitors to provide information on their data protection measures.

Could I get compensated?

It's possible. Class-action complaints are piling up fast, with about two dozen filed within a few days of the exposure's revelation.

Chances are the company may eventually offer a settlement, pay government fines, or both.

Has the company apologized?

Yes. Equifax CEO Richard F. Smith [apologized Tuesday in a USA TODAY op-ed](#) and said the company initially "thought the intrusion was limited" after discovering it on July 29.

Follow USA TODAY reporter Nathan Bomey on Twitter [@NathanBomey](#).