EQUIFAX DATA BREACH: WHAT YOU NEED TO KNOW

On Friday, Equifax, one of the major credit reporting bureaus, issued a press release announcing that on July 29 it had discovered “unauthorized access” to data belonging to as many as 143 million U.S. consumers. We have compiled some information that we hope may help you understand what happened and what to do next. As always, please don’t hesitate to reach out to us if you have specific questions.

Equifax has stated its internal investigation determined no evidence of unauthorized activity on its core consumer or commercial credit reporting databases. However, the data accessed includes names, Social Security numbers, birth dates, addresses and, in some cases, driver’s license numbers. In addition, credit card numbers were accessed for approximately 209,000 U.S. consumers and personal identifying information on documents for another 182,000 people.

Equifax has set up a **website** on which you can enter your last name and the last six digits of your Social Security number to see if you have been affected by the breach.

Many people using this website have received error messages, perhaps due to the volume of people accessing it. Unfortunately, at this time, the results provided by the website can be vague and not necessarily reliable. Considering that the 143 million U.S. consumers affected represent 55 percent of the adult U.S. population over the age of 18, we recommend that you act as if your information was accessed as part of this data breach.

YOUR NEXT STEPS

Free enrollment is being offered in the identity protection program TrustedID Premier, a three-bureau (Equifax, Experian and Trans Union) credit monitoring service run by Equifax. Anyone can enroll in this program at no charge – regardless of whether their information was accessed – through Nov. 21, 2017.

A few things to keep in mind regarding this offer:

- Initially, arbitration language applying to those who choose to enroll in an Equifax credit monitoring program appeared to potentially prohibit them from participating in any class action lawsuits that might result from this data breach. On Sunday evening, Equifax issued a statement saying: “Enrolling in the free credit file monitoring and identity theft protection products that we are offering as part of this cybersecurity incident does not prohibit consumers from taking legal action." Equifax has since removed the arbitration language from the terms of use on its **data breach notification website**.
- Credit monitoring services, such as the one being offered by Equifax, do not prevent thieves from stealing your identity. What they can do is alert you that your identity has been stolen and, in some cases, be helpful in recovering from identity theft.

RECOMMENDATION

In conjunction with credit monitoring (either via a monitoring service or on your own by periodically requesting a credit report), place a security freeze on your credit files.

Note: Typically, once a credit freeze is in place, you can’t sign up for a credit monitoring service. The order in which you take these steps is important if you choose to do both.

The following are some frequently asked questions about security credit freezes:

What does a security freeze do?

A security freeze blocks potential creditors from seeing your credit file while it is in place. Therefore, an identity thief who has your information has no way of gaining new lines of credit because a creditor won’t issue one without being able to see your current credit score and file.

How do I put a security freeze in place?

You will need to notify four credit bureaus – Equifax, Experian, TransUnion and Innovis. This notification can typically be done online. Once completed, each bureau will provide you with a PIN to be used to unfreeze or "thaw" your credit file when you need to apply for new lines of credit.

Many states allow you to do this at no charge, but some states charge a nominal fee – typically up to $15 – for each credit freeze per bureau.

What is the advantage of a security freeze over a fraud alert?

A fraud alert is good for only 90 days, but can be renewed. Alternatively, you can get an extended fraud alert, which lasts for seven years.

When you have a fraud alert in place, lenders and service providers are expected to contact you for approval before issuing any new line of credit. A key point regarding fraud alerts is that lenders and service providers are supposed to receive your permission before granting new lines of credit in your name, but they are not legally required to do so.

OTHER TIPS

The Equifax data breach is an unfortunate reminder of how valuable your data and personal information is, and an opportunity to revisit what you can do to protect yourself:

- Do not send personal, confidential information, including your financial account numbers, Social Security number or passwords, through email. Regardless, always use an email encryption service.
- Review your credit card and bank statements each month for any suspicious transactions or activity.
- Most identity theft occurs via phishing emails in which the end user is tricked into clicking on links or providing information that allows fraudsters to gain access to accounts or personal information.
- Use string passwords and don't default to the same password multiple times. If you have a lot of passwords, this can be difficult. Consider using password management software.

For more general information about how to protect against fraud, we recommend visiting the Federal Trade Commission's ***consumer information website****.*