EQUIFAX BREACH

Consumer Alert

What You Need to Know About the Equifax Breach

In the news:

Criminals gained access to Equifax's database from mid-May through July 2017. The breach impacted the social security numbers, birth dates, and addresses of 145.5 million Americans, including more than 4.6 million Michigan residents.

Credit card information, dispute documents with personal identifying information, and driver's license numbers were also stolen in some cases.

What you need to know:

When breaches, like this one, occur from hacking or unauthorized access, the stolen personal information is more likely to be used to commit identity theft. Thus, you need to take the threat seriously and take steps now to prevent becoming an identity theft victim.

First, some red flags:

Starting February 1, 2018, Equifax will no longer offer its TrustedID products, but will instead offer a "Lock & Alert" service to control access to your Equifax credit report. Equifax is advertising that the service is "free, for life." Credit card information is not required to enroll.

If you checked your breach status before Oct. 8, 2017, and you were not impacted, you should check again since 2.5 million additional impacted consumers were identified in early October, including almost 80,000 more Michigan residents; and another 2.4 million consumers were identified in March 2018 whose partial driver's license information was stolen.

What you can do:

Take these steps to help prevent identity theft:

1. Before entering any information online, make sure that you are on a safe connection (look for the https) and do not use public Wi-Fi or a public computer, since both can put you at additional risk for identity theft.

2. Go to Equifax's Cybersecurity Incident & Important Consumer Information website (equifaxsecurity2017.com) to see if your information has been impacted.

   Read Equifax's FAQ for Consumers; Progress Updates for Consumers; and Notice of Data Breach.

3. Place a security freeze on your credit file at each of the three major credit reporting agencies.

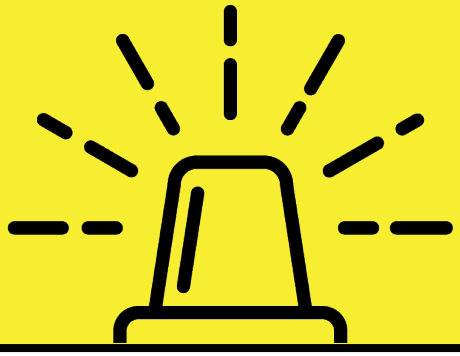
For extra security, you can apply a freeze to a fourth, lesser-known agency, Innovis.

Freezing your credit reports is an effective way to prevent identity theft. With a security freeze, you and a select few others are the only ones that can access your information. Security freezes require a PIN and placing them on your reports will not affect your credit score.

Starting June 17, 2018, credit reporting agencies may not charge Michigan residents a fee to place or to temporarily or permanently lift a security freeze.

In the meantime, Equifax has extended the deadline for FREE security freezes to June 30, 2018.

Bill Schuette
Attorney General



EQUIFAX BREACH

Consumer Alert

Credit Reporting Agency Contact Information:

Equifax
P.O. Box 740241
Atlanta, GA 30374
equifax.com
**See phone numbers below*

TransUnion
P.O. Box 2000
Chester, PA 19016
transunion.com
800-680-7289

Experian
P.O. Box 9554
Allen, TX 75013
experian.com
888-397-3742

Innovis
P.O. Box 1640
Pittsburgh, PA 15230
innovis.com
800-540-2505

*Equifax has different numbers to contact to accomplish the following:

- **Determine an information breach or help with TrustedID Premiere:** 888-548-7878
- **Place a fraud alert:** 888-766-0008
- **Place a credit freeze:** 800-685-1111
- **General Qs about the 2017 breach:** 866-447-7559

For more information on initial fraud alerts and security freezes, review the Attorney General's Consumer Alert, Credit Freeze; Fraud Alert; & Credit Monitoring.

4. Place an initial fraud alert on your credit file. Once you receive notice of a security breach, federal law provides you with a free and easy way to minimize the risk of fraud.

   An initial fraud alert is a free alert, or flag, that is placed on your credit file when you notify a credit reporting agency that your information may have been compromised. This alert will make it more difficult for anyone to open an account in your name. The Federal Trade Commission provides a checklist for this.

   There are three important things to keep in mind when placing an initial fraud alert on your file: 1) the alert makes it more difficult for anyone, including yourself, to open an account in your name; 2) when someone attempts to open or extend credit in your name the creditor is required to take additional steps to try to verify that you have authorized the request; and 3) the initial fraud alert will only stay on your file for 90 days.

   Federal law requires that the credit reporting agencies provide you with a free copy of your credit report after you place a fraud alert, and it requires the credit reporting agency that you contact to notify other nationwide credit reporting agencies. Innovis is not a nationwide agency and must be notified separately.

   Be sure to review your credit report carefully, to ensure that there is no inaccurate information in your file and that no fraudulent accounts have been opened in your name.

5. Consider taking advantage of any **unconditional** and free subscription to any credit monitoring, fraud resolution, or other service designed to protect and help you. Credit monitoring services will alert you if there are any changes to your credit report. That said, credit monitoring does not necessarily prevent identity theft.

   Most credit monitoring services simply monitor a consumer's credit report and notify the consumer if there are changes. Consumers must act to take further protections.

Before you accept a free subscription offered to you as a result of a security breach, carefully consider any conditions placed on your acceptance of this subscription.

For example, will you be charged after a short free period? Or will you only get the free subscription if you give up your right to additional legal redress?

EQUIFAX BREACH

Consumer Alert

If you signed up for TrustedID:

Your TrustedID services will end one year from the date you signed up for them, and include:

1. Equifax Credit Report
2. Bureau Credit File Monitoring
3. Equifax Credit Report Lock
4. Social Security Number Monitoring
5. $1 million Identity Theft Insurance

Before you sign up for Lock & Alert:

- Carefully consider all of the terms of service.
- Review the privacy policy to learn if any of your information will be shared.

More things you can do:

- Monitor your financial accounts (credit cards, banking, utilities, and etc.) monthly for any signs of fraudulent activity.
- Stay alert for notifications about potential fraud occurring due to the data breach.
- Be aware of phishing attempts exploiting the data breach to get you to click on a link in an email or share your personal information.
- If your driver's license is stolen, you can go into a Secretary of State office with other identification documentation and ask for a "stolen flash" to be placed on your record.
- Use two-factor authentication for all of your online accounts.
- File your taxes early to avoid refund fraud.
- Educate yourself about the different types of identity theft, including: financial identity theft; governmental identity theft; criminal identity theft; medical identity theft; and child identity theft.

Additional Resources on Identity Theft Prevention and Resolution:

Additional information on identity theft prevention and resolution for Michigan consumers is available on the Attorney General's website.

Michigan consumers may visit the Federal Trade Commission's website devoted to identity theft.

Michigan consumers may also call the Federal Trade Commission's ID Theft Hotline, at 877-ID-THEFT (438-4338); or seek help at the Identity Theft Resource Center, 888-400-5530.

For general consumer questions or complaints, you may reach the Attorney General's Consumer Protection Division at:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-373-1140
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form

Bill Schuette
Attorney General