What to Do In Response to the Equifax Data Breach

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

Last fall, Equifax, a major national credit bureau, announced a massive data breach affecting approximately 148 million consumers nationwide. Hackers stole highly sensitive information, including Social Security numbers, birth dates, addresses, and some driver's license numbers. The company indicates that data on over 2 million Minnesota residents was compromised.

People can take the following steps to protect against identity theft as a result of Equifax's data breach:

Steps To Take to Protect Yourself

- Carefully monitor your credit reports and financial accounts for unauthorized activity and immediately alert your financial institution and local law enforcement of any suspicious activity. You can request a free copy of your credit report once each year by any of the following methods:
  1. Log on to: *www.AnnualCreditReport.com*;
  2. Call: (877) 322-8228; or
  3. Write: Annual Credit Report Request Service at P.O. Box 105281, Atlanta, GA 30348-5281.

  Please note that the credit bureaus all offer fee-based products where you can pay to get a credit report. There are also scam websites that pose as credit bureaus. You should avoid these websites and only order your free credit report by the above-described methods.

- Consider placing a fraud alert on your credit reports, which requires creditors to contact you before opening any new accounts or increasing your credit limit. To do so, call any one of the three major credit bureaus at the following numbers:
  1. Experian: (888) 397-3742;
  2. TransUnion: (800) 680-7289; or
  3. Equifax: (800) 525-6285.

  The fraud alert will remain in your credit file for at least 90 days. Starting on September 21, 2018, a new law provides that fraud alerts will remain in your file for at least 1 year.

- Consider placing a security "freeze" on your credit reports by contacting each of the three major credit bureaus. This is supposed to prevent the release of any information from your credit report without your written authorization, which makes it more difficult for identity thieves to open new accounts (but also harder for you to quickly open a new account). For more information on how to place a credit freeze, you may download our brochure, entitled *Protect Yourself from Identity Theft* available at *www.ag.state.mn.us/Office/Publications.asp*.

  There is no cost for placing a security freeze on your credit reports. Starting on September 21, 2018, a parent or guardian may freeze the credit file of a child under 16 for free as well.

- If you suspect someone is misusing your Social Security number (SSN), report the problem to the Social Security Administration at (800) 772-1213. If someone uses your SSN to commit fraud, you should immediately report the fraud to the Social Security Fraud Hotline at (800) 269-0271, and the Internal Revenue Service's Identity Protection Specialized Unit at (800) 908-4490.

Additional Information Through Equifax

Equifax has a website, *www.equifaxsecurity2017.com*, which provides additional information and resources about the data breach. At this website, you may check if your personal information was exposed as part of the data breach. To do so, you must submit your last name and the last six digits of your Social Security number.

At this website, you may also enroll in Equifax's free "Lock & Alert" product, which allows you to lock and unlock your Equifax credit file for free. You should be aware that a "lock" is similar to the credit "freeze" described above, but the lock does not contain all of the same protections as a credit "freeze," which is governed by state law. Lock & Alert does not freeze or lock your Experian or TransUnion credit files.

Imposter Scams

Equifax has indicated that it will not email, text, or call Minnesota residents to notify them that their personal information was exposed by its data breach. If you receive emails, texts, or calls from any person or company claiming to be Equifax or anyone else related to the data breach, they are probably an imposter scam. You should not open or respond to such communications. Communicating with such scam artists, even to ask them to stop contacting you, may only encourage them to continue contacting you.

Additional Resources

For more information, the Minnesota Attorney General's website at *www.ag.state.mn.us* has publications entitled:

1. *What to Do When Your Personal Information is Breached;*
2. *Protect Yourself from Identity Theft; and*
3. *Guarding Your Privacy.*

They are downloadable from the site at *www.ag.state.mn.us/Office/Publications.asp.*