Protecting Your Identity

FIDUCIARY™ TRUST

Information Security Insights

All too frequently, we see headlines about data breaches of personal information. The recent theft of Equifax's information on over 140 million consumers is particularly concerning due to the size of the breach and the types of information accessed, which included Social Security numbers.

To see if your information is at risk as a result of the Equifax breach, you may check the special website they have established – it requires entering your name and the last six digits of your Social Security number. Remember to only enter a Social Security number online if you are using a secure internet connection on a computer that has up-to-date virus protection software.

What Should You Do?

In the case of credit card number theft, credit card issuers are often proactive by automatically changing card numbers. They may also offer credit monitoring services. With other types of security breaches, immediate actions the institution can take may be more limited. The following are some steps you can take to help protect yourself, regardless of whether your information has been part of a data breach:

1. **Check Your Credit Reports.** Review your credit reports for accounts or activity you do not recognize. Contact the financial institution(s) issuing the credit if the information appears unfamiliar. You are entitled to one free credit report per year from each of the three credit reporting agencies (Equifax, Experian and TransUnion). You can access your reports at annualcreditreport.com.
2. **Monitor Your Existing Accounts.** Regularly check your credit card and bank statements for charges or transfers you do not recognize, and notify your bank immediately if there are items that appear to be fraudulent. You should also file a report with your local police if someone has stolen your identity and committed fraud.

Learn More:

For more information on Fiduciary Trust visit:

www.fiduciary-trust.com

or contact:

Rick Tyson
tyson@fiduciary-trust.com
617-292-6799

Author

Robert J. Jeffers
Chief Operating Officer

Learn More:

For more Fiduciary Trust Insights visit:

www.fiduciary-trust.com/insights

3. **Protect Online Account Access.** Use long, difficult-to-guess passwords and multi-factor authentication for your online bank and other accounts, where available. (Multi-factor authentication generally refers to logging into an account using an ID, password and a one-time use number delivered via text message or email). Change your passwords immediately if you believe you are a fraud victim or your password may have been compromised.
4. **Consider Freezing Your Credit Report Account.** A credit freeze prevents the credit agencies from providing your credit history to financial services institutions, except for your existing service providers, making it very difficult for someone to open new credit in your name. The freeze will not prevent someone from using your existing credit cards and other credit facilities.

   To freeze your credit, contact each of the credit agencies online or via phone and request a freeze: Equifax (800-349-9960), Experian (888-397-3742) and TransUnion (888-909-8872). Note that you will likely have to unfreeze your credit report to obtain new credit. You may also need to unfreeze it to setup new utilities, rent an apartment, obtain an insurance policy or apply for a job. There is also a minor cost, typically $5 to $10, each time you freeze or unfreeze your account with each credit reporting agency (unless you are the victim of identity theft, in which case it is usually free). Remember to keep the PIN associated with your credit freeze in a safe place.
5. ***If You Do Not Freeze Your Credit Report:* Consider Placing a Fraud Alert on Your File and Opt-out of Pre-screened Credit Offers.** The fraud alert warns creditors that you may be the victim of fraud and to take extra precautions to verify your identity before issuing credit. If you are not an actual victim of fraud, the alert will expire after 90 days (otherwise it will remain on your file for seven years). If you set the alert with one agency, they are required to notify the other two.

   You can further reduce your exposure to identity theft by opting out of unsolicited credit card or insurance offers by going to www.optoutprescreen.com, or calling 888-5OPT-OUT.
6. **File Your Taxes Early.** One of the ways criminals have used stolen personal information is through filing fraudulent tax returns and requesting refunds. You can reduce the potential for this theft by filing as early as is practical.

   Fiduciary Trust takes information protection seriously and employs a number of safeguards and ongoing testing to help keep client and other information secure. See our related article, “Cybersecurity: Reducing Your Risks,” for other recommendations on how to protect your personal information.

FIDUCIARY™ TRUST