Excerpts from the Consumer Financial Protection Bureau website posting

# "Top 10 ways to protect yourself in the wake of the Equifax data breach"

by Kristin Dohn, September 18, 2017.

## Top 10 ways to protect your personal information from being misused

**1. Review your credit report.** You are entitled to a free credit report every 12 months from each of the three major consumer reporting companies (Equifax, Experian and TransUnion). You can request a copy from AnnualCreditReport.com .

**2. Consider a security freeze.** A security freeze or credit freeze on your credit report restricts access to your credit file. Creditors typically won't offer you credit if they can't access your credit reporting file, so a freeze prevents you and others from opening new accounts in your name. In almost all states, a freeze lasts until you remove it. In some states, it expires after seven years.

**3. Set up a fraud alert.** Fraud alerts require that a financial institution verifies your identity before opening a new account, issuing an additional card, or increasing the credit limit on an existing account. A fraud alert won't prevent lenders from opening new accounts in your name, but it will require that the lenders take additional identification verification steps to make sure that you're making the request. An initial fraud alert only lasts for 90 days, so you may want to watch for when to renew it. You can also set up an extended alert for identity theft victims, which is good for seven years.

**4. Read your credit card and bank statements carefully.** Look closely for charges you did not make. Even a small charge can be a danger sign. Thieves sometimes will take a small amount from your checking account and then return to take much more if the small debit goes unnoticed.

**5. Don't ignore bills from people you don't know.** A bill on an account you don't recognize may be an indication that someone else has opened an account in your name. Contact the creditor to find out.

**6. Shred any documents with personal or sensitive information.** Be sure to keep hard copies of financial information in a safe place and be sure to shred them before getting rid of them.

**7. Change your passwords** for all of your financial accounts and consider changing the passwords for your other accounts as well. Be sure to create strong passwords and do not use the same password for all accounts. Don't use information such as addresses and birthdays in your passwords. For more tips on how to create strong passwords read more on the Federal Trade Commission's (FTC) blog .

**8. File your taxes as soon as you can.** A scammer can use your Social Security number to get a tax refund. You can try to prevent a scammer from using your tax information to file and steal your tax refund by making sure you file before they do. Be sure not to ignore any official letters from the IRS and reply as soon as possible. The IRS will contact you by mail; don't provide any information or account numbers in response to calls or emails.

**9. Active duty servicemembers are eligible for additional protections**, and should also monitor their credit carefully. Learn more about what you can do if you're currently serving at home or abroad.

**10. If you are the parent or guardian of a minor** and you think your child's information has been compromised, here are some steps from the FTC you can take to protect their information from fraudulent use. If you think you or your child's identity has already been stolen you can follow checklists and additional steps provided by the FTC to begin recovering from a case of identity theft.