Equifax Data Breach - What Now?

Are you wondering what to do after the Equifax Security Breach? Well honestly, so am I! This is the first security breach that has exposed essentially all the components at one time that an identity thief needs to commit a variety of crimes using your information. Because the hacked information includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers, the steps to protect yourself will not be easy or quick. I expect that we will continue to see new recommendations regularly as the scenario plays out in the coming months (and maybe years). But for the moment, let's look at what a thief can do with your information and possible steps to take:

1. **Steal Your Information** – Thieves might steal your personal information to either sell it to others or use it themselves to commit a variety of crimes. *Check to see if Equifax thinks your information was compromised and to sign up for one year of free credit monitoring (available whether or not your information was compromised). Sign up for credit monitoring **before** freezing your credit.*

www.equifaxsecurity2017.com (Equifax Security Breach Site)

2. **Commit Existing Account Fraud** – The thief may use your existing credit card, bank account, internet payment account, etc. to get money or pay for items they receive. *Monitor your accounts carefully, checking every transaction to be sure that it is yours. Report all suspicious transactions, even very small ones. Set alerts on your accounts, so that you will be notified of transactions and can spot unusual activity. Find out about fraud/security protections of your 401(k) or other investment plan company.*

3. **Commit New Account Fraud** – The thief may open a new credit card account, bank account, internet payment account, wireless service, or auto, personal, or student loan in your name. *Opt out of pre-approved credit offers. Consider fraud alerts and/or freezes at each of the credit reporting agencies and bank account verification agencies:*

www.optoutprescreen.com (Opt-out of pre-approved credit offers.)
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp (Equifax Freeze)
https://www.experian.com/freeze/center.html (Experian Freeze)
https://www.transunion.com/credit-freeze/place-credit-freeze2 (Trans Union Freeze)
https://www.innovis.com/personal/securityFreeze (Innovis Freeze)
www.chexsystems.com (Chexsystems Freeze – Click on "Security Freeze" on the menu.)
https://www.firstdata.com/telecheck/telecheck-file-report.html (Request Telecheck report - no freeze information listed.)
https://www.earlywarning.com/consumer-information.html (Request Early Warning report - no freeze information listed.)
https://www.askcertegy.com/FACT.jsp (Request Certegy report - no freeze information listed.)

4. **Commit Criminal Identity Theft** – The thief may use your name and information during interactions with law enforcement, leading to arrest warrants or court proceedings in the victim's name. *(Seek professional/legal advice if this occurs.)*

5. **Commit Employment Identity Theft** – The thief may get a job using your name and Social Security number. *Activate your Social Security account online to confirm the accuracy of your earnings and benefits statement. Periodically check to be sure that only your own earnings are being reported. A security freeze at Equifax will block the ability to set up an SSA account online, but will not affect existing accounts. If you already have an account, consider blocking electronic access to at the link listed below.*

www.ssa.gov
www.socialsecurity.gov/blockaccess (Block all electronic access to your Social Security information.)
https://blog.ssa.gov/protecting-your-social-security/

6. **Commit Medical Identity Theft** – The thief may use your information to get access to health care. *Sign up for an online account through your insurer. Monitor your health care accounts and statements carefully. Report any medications, treatments, or providers that are not consistent with care you have received.*

7. **Commit Mortgage Fraud** – The thief may get a mortgage in your name or pose as your home's owner to get the deed transferred into his/her own name. *See new account fraud above.*

8. **Commit Synthetic Identity Theft** – The thief might use your Social Security number in combination with another person's name and birthdate to create a new, fictitious identity. *Monitor your Social Security records for possible fraudulent activity.*

9. **Commit Tax Fraud** – The thief might file a tax refund in your name to receive a refund or other funds owed to you. *File your taxes as early in the year as possible. Adjust your withholding so that you get the smallest refund possible, in case a thief does try to steal your refund. File an Identity Theft Affidavit with the IRS to flag your account for extra monitoring.*

Yes, all of this is scary. I understand what you are going through because the information of everyone in my immediate family was compromised in this breach. My intent is not to cause fear, but to encourage vigilance. We will be wise to take the actions that are recommended today and in the coming weeks. But we can't stop there. We will need to carefully check every statement we receive, request and review every consumer report that is available to us, and verify the credibility of every request for personal information we receive, probably for the rest of our lives. Nothing we can do is guaranteed to prevent a thief from committing these crimes. However, the sooner we notice a problem, the better our chances to resolve it before it becomes a nightmare.

Other Articles and Resources:
http://articles.extension.org/pages/74535/data-breaches-credit-freezes-and-vigilance
https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
https://www.identitytheft.gov/
https://www.fcc.gov/smartphone-security
http://www.idtheftcenter.org/equifaxdatabreach
https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf

Written by:
Karen Lynn Poff, MPA, AFC®, Senior Extension Agent, Family and Consumer Sciences
Virginia Cooperative Extension – Northern Shenandoah Valley Financial Education Program
220 North Commerce Avenue, Suite 500
Front Royal, VA 22630-3495
Phone: 540/635-4549 Fax: 540/635-2827
E-mail: kpoff@vt.edu
LinkedIn: www.linkedin.com/in/karenlynnpoff
NSV Financial Education Website – http://warren.ext.vt.edu/programs/nsvfep.html
NSV Financial Education Facebook Page – https://www.facebook.com/nsvfinancialeducation