Life after the Equifax Hack

On September 7th, Equifax announced that their network was hacked from mid-May through July 2017. They discovered the incident at the end of July. More than 143 million records may be compromised. Equifax believes the stolen information includes names, Social Security numbers, addresses, birth dates and, in some instances, driver's license numbers and dispute documents.

While news of hacking and data breaches can seem almost routine, it is hard to overstate the significance of this crime. If your credit card information was stolen when a retailer like Target was hacked, the account could be closed. Validated SSNs, birth dates and full names necessary to open new credit cards and other financial accounts are a much bigger problem.

It is likely that some new regulations will emerge from this incident, but it is important to act to protect yourself.

- **Consider your information hacked regardless of any indication from Equifax.**
- **Be cautious online. Fraudsters are registering phony website names hoping you will reach the wrong one.** Start from the main company website, e.g. www.equifax.com or spend time to verify that a site such as www.equifaxsecurity2017.com/ is authentic.
- **Check your own credit report more often than the once/year opportunity that the U.S. government requires each agency to provide** for free via http://www.annualcreditreport.com/. If someone opened accounts in your name without your authorization the FTC offers guidance on steps to take at www.IdentityTheft.gov.
- Consider a monitoring service, but don't expect it to stop fraud or identity theft. Equifax is offering their service free for a year, but you may consider services from the other agencies or your credit card companies if you feel like you would renew it in a year and prefer not to reward Equifax. Equifax has

recently stated that it will not apply the arbitration language in the terms that would have affected legal rights of anyone subscribing through them.

- **Consider credit freezes on your files** to make it harder for someone to open a new account in your name. This will not stop someone from changing an existing account. You may be required to pay to freeze/unfreeze and renew the freeze. Costs vary by state and you will need to keep the security code or PIN in a safe place. The U.S. Federal Trade Commission has additional information about credit freezes here: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

  - **Equifax** https://help.equifax.com/app/answers/detail/a_id/75/search/1
  - **Experian** https://www.experian.com/freeze/center.html
  - **Trans Union** http://www.transunion.com/securityfreeze
  - **Innovis** https://www.innovis.com/personal/securityFreeze

- Secure **your email account** (more info below).

- Be alert for new email and telephone scams coming from fraudsters who may already have some of your personal information. The FTC notes that imposters may use your Social Security number to get a job or tax refund in your name and recommends responding right away to letters from the IRS.

- Educate your family about online and financial safety. The FTC offers educational videos at https://www.consumer.ftc.gov/media.

As much as your credit history and files matter to your financial identity, email accounts and cell phones have become central to the process. We cannot recommend enough that everyone invest the time to learn and adopt secure settings to prevent hackers from accessing your email and/or phone and intercepting messages and/or taking control your account.

We do not recommend a particular email solution, but if your email provider does not have options for multifactor\authentication or you do not use a corporate account with dedicated security, you may want to find another provider. Most providers have guidance for adopting enhanced security; some of the most popular are:

Gmail https://myaccount.google.com/intro/security

Outlook.com/Hotmail https://www.microsoft.com/en-us/safety/pc-security/webmail.aspx

Yahoo https://help.yahoo.com/kb/account/secure-yahoo-account-sln2080.html?impressions=true

Nor do we recommend a particular cell phone solution, but it's noteworthy that Google followed Apple and developed their own phone hardware. They had both financial *and* security reasons. Mobile carriers can be slow to push updated and patched operating systems. If you use a mobile device to access email or conduct financial transactions it should be updated and fully patched. If it is no longer possible to update your device you may need to upgrade or limit how you use your phone, possibly even turning off significant features like Bluetooth to protect yourself from vulnerabilities such as BlueBorne (https://www.kb.cert.org/vuls/id/240311).

If you have concerns that someone may be using your information for fraudulent purposes, or has hacked your phone or email, please review the FTC's guidance at www.IdentityTheft.gov and contact us so that we can increase our vigilance even further.

Please send your questions, comments and feedback to: info@mai.capital. Opinions expressed herein reflect the author's judgment and are subject to change without notice based on legal and government policy conditions.