NORTHERN TRUST

PROTECTING YOUR IDENTITY AFTER A BREACH

WHAT TO DO IF YOU SUSPECT YOUR PERSONAL INFORMATION MAY HAVE BEEN COMPROMISED

August 2019

The world we live in is full of potential threats, particularly when it comes to cybersecurity and protecting your personal information. On July 29, 2019, a major financial service company reported a cybersecurity incident involving consumer information impacting approximately 100 million U.S. citizens. In addition, on July 22, the Federal Trade Commission and Equifax reached an agreement for Equifax to pay at least $575 million and up to $700 million to compensate those whose personal data was exposed with the breach of the Equifax servers in 2017. With these and other stories in the news, it's not uncommon to have questions. Rest assured — even when you know your information is at risk, there are still things you can do to help protect yourself from lasting damage.

If your personal data was exposed in the 2017 Equifax data breach, you may be eligible for part of the $700 million settlement. According to the Federal Trade Commission, consumers whose information was exposed can submit a claim for up to $125 or up to 10 years of free credit monitoring. To reduce the risk of entering information into a fake website, use *only* the link from the Federal Trade Commission at www.ftc.gov.

RECOMMENDED PRACTICES:

- Be vigilant, monitor all financial accounts regularly and take advantage of all alerts to track activity. If you do not have access to free credit monitoring, proactively check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year.
- If the company responsible for exposing your information offers you free credit monitoring, take advantage of it. Your credit report is one of the best tools you have available to identify potential issues before they get out of control.
- Consider signing up for a credit monitoring service on your own — such as LifeLock, Identity Guard and Identity Force — which offer a variety of comprehensive plans ranging from alerts to "family" coverage, which will monitor your children's Social Security numbers in addition to your own.
- Change your passwords. Passwords should be changed on all of your sensitive financial accounts at least once every 30 to 90 days.

- Implement two-factor authentication whenever possible — on your personal email, LinkedIn, PayPal, online bank accounts, etc.
- Consider using LastPass, Dashlane, Sticky Password or another similar product to store and protect your passwords.
- As a reminder, for banking clients, transaction alerts can be added to Private and Treasury Passports for real time information relating to account activity.

EXTRA PRECAUTIONS

- Placing a "fraud alert" on your credit accounts can be an option. According to Transunion, "a fraud alert is a cautionary flag, which is placed on your credit file to notify lenders and others that they should take special precautions to verify your identity before extending credit." Fraud alerts may be as simple as providing a mobile or other phone number for a lender to contact you to verify that the account activity or application is really from you, and not from a cybercriminal. A fraud alert can be placed with one of the three major credit reporting agencies and will carry over to the others with no further action on your part. Fraud alerts tend to last 90 days and then expire.
- Many experts are recommending a "credit freeze," also known as a "security freeze." Although a credit freeze can cause delays in opening new accounts and in obtaining loans/credit line increases in the short term, this tool allows you to restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name — including actually extending credit to you. Placing a security freeze will prevent lenders and others from accessing your credit report entirely. With a security freeze in place, you will need to take special steps when you wish to apply for any type of credit. Note that because of more stringent security features, you will need to place a security freeze separately with each of the three major credit reporting companies. A security freeze remains on your credit file until you remove it or choose to lift it temporarily.

As always, the best protection against identity theft is vigilance. Monitoring your bank, credit and investment accounts for unusual activity and contacting the appropriate parties as soon as you notice something is wrong is crucial to avoiding major problems down the line. For more tips on improving your personal security, contact your relationship manager or visit the Security Center on northerntrust.com.

One of the easiest ways to see if a criminal is fraudulently using your identity is to review your credit report. The Fair Credit Reporting Act (FCRA) requires each of the nationwide credit reporting companies — Equifax, Experian and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months.

The Federal Trade Commission has an excellent website including information about the recent breaches. Visit the FTC at www.ftc.gov.