PROTECTING YOUR IDENTITY AFTER A BREACH

What to do if you suspect your personal information may have been compromised.

September 8, 2017

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.

If you received a notice that says your personal information was exposed in a data breach – or you've simply lost your wallet or your Social Security card – you probably have questions and concerns. Rest assured – even if you're sure your information is at risk, there are still things you can do to help protect yourself from lasting damage.

START WITH THE BASICS

- 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. Should you notice a discrepancy, take advantage of the "dispute", "freeze" and "fraud alert" services offered.
- Consider signing up for a credit monitoring service on your own – services such as Lifelock, Identity Guard or Identity Force offer a variety of comprehensive services 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 thirty days.
- Implement 2-step authentication whenever possible - on your personal email, your mobile service provider, your bank accounts, etc.
- Be vigilant for Phishing (email scams) and Vishing (phone scams) which may increase in volume and sophistication after an event. Phishing scams offering "protection" or remediation are common. Do not respond to unsolicited offers for assistance from merchants, instead, initiate contact with legitimate service providers.
- Consider using LastPass, Dashlane, Sticky Password or another similar product to store and protect your passwords.
- Consider using a separate computer or mobile device for your financial business that is unrelated and isolated from the devices used for games, movies, and browsing.

FRAUD ALERT/CREDIT FREEZE

- 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.

- A more drastic step is a Credit or Security Freeze. Placing a Security Freeze will prevent lenders and others from accessing your credit report entirely. This will prevent anyone from extending credit in your name – including actually extending credit to you. 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 northerntrust.com/securitycenter.