WHAT YOU NEED TO KNOW ABOUT THE EQUIFAX BREACH

September, 2017

Last week, credit reporting agency Equifax disclosed a breach of consumer information resulting from a cybersecurity incident that impacts approximately 143 million U.S. consumers. According to Equifax, cyber criminals exploited a website application vulnerability allowing them to gain access to a limited number of files. The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personally identifying information for approximately 182,000 U.S. consumers, were accessed.

At this time Northern Trust is not aware of any occurrences of this nature against our bank, and has no reason to believe that any Northern Trust company or client data or assets are at increased risk.

What steps should I take to protect myself and my family?

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 in the future.

Immediate Actions:

At this point, take action with the assumption that your information was compromised.

Step One: Proactively check your credit reports at www.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.

Step Two: Change your passwords. Passwords should be changed on all of your sensitive financial accounts at least once every sixty to ninety days.

Step Three: Implement 2-factor authentication whenever possible - on your personal email, your mobile service provider, your bank accounts, etc. Visit www.turnon2fa.com for step-by-step instructions explaining how to enable two-factor authentication for many popular sites, including social media, financial accounts, shopping accounts, and more.

Step Four: Review and consider changing 'challenge response answers' that may use responses containing information that is easily obtainable (such as from Social Media Accounts) or that could have been exposed in the Equifax breach.

Step Five: Consider signing up for a credit monitoring service on your own – services such as Lifelock, Identity Guard or Identity Force offer a variety of services ranging from alerts to "family" coverage to cyber insurance. For example, LifeLock offers some personal expense compensation, reimbursement of stolen funds, and coverage for legal and/or expert fees depending on the plan you purchase. Other plans, such as Credit Karma, are free and offer no cost monitoring.

Step Six: Set up alerts on your financial accounts and monitor your accounts DAILY. Most financial institutions will allow you to set up alerts to notify you if charges are made online, if charges exceed a certain threshold, or if charges are made internationally. In many cases, these alerts are real-time and will allow you to receive instant notification of activity on your accounts. If the activity is not legitimate, you are then able to take action immediately to remediate or potentially block the transaction in question.

Should I do Fraud Alert or 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.

Ongoing Actions:

- 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.

For more tips on improving your personal security, contact your relationship manager or visit Security Center | Northern Trust.