



First National Bank and Trust Company has been safeguarding our customers' information long before identity theft became an issue. Our employees are educated about protecting personal information. We will gladly answer any questions you might have about the safety of your personal information or protecting your financial identity.

As most of you have heard there was a cybersecurity breach with Equifax. This was NOT a compromise of First National Bank and Trust Company, and no information was taken from our systems. If you have a credit report there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

**Below is important information regarding this extensive breach with links to additional information to assist our customers.**

**Here are the facts, according to Equifax.**

- The breach lasted from mid-May through July.
- The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.
- They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. And they grabbed personal information of people in the UK and Canada too.

**There are steps to take to help protect your information from being misused. Visit Equifax's website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com).**

- Find out if your information was exposed. Click on the "Potential Impact" tab and enter your last name and the last six digits of your Social Security number. Your Social Security number is sensitive information, so make sure you're on a secure computer and an encrypted network connection any time you enter it. The site will tell you if you've been affected by this breach.
- Whether or not your information was exposed, U.S. consumers can get a year of free credit monitoring and other services. The site will give you a date when you can come back to enroll. Write down the date and come back to the site and click "Enroll" on that date. You have until November 21, 2017 to enroll.
- You also can access [frequently asked questions](#) at the site.

## Here are some other steps to take to help protect yourself after a data breach:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting [annualcreditreport.com](http://annualcreditreport.com). Accounts or activity that you don't recognize could indicate identity theft. Visit [IdentityTheft.gov](http://IdentityTheft.gov) to find out what to do.
- **Consider placing a [credit freeze](#) on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.
- **File your taxes early** — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- **Check if you are affected** and regardless, enroll in the free identify protection offered by Equifax: <https://trustedidpremier.com/eligibility/eligibility.html>
- **Monitor you bank account** for fraudulent activity
- If you decide against a credit freeze, **consider placing a [fraud alert](#) on your files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

- **Federal Trade Commission**, Consumer Response Center [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)
- **State Attorneys General:** Information on how to contact your state attorney general may be found at [www.naag.org/naag/attorneys-general/whos-my-ag.php](http://www.naag.org/naag/attorneys-general/whos-my-ag.php).

Please contact Equifax for specific questions about the Equifax breach and its effect on your information. Equifax has set up a dedicated call center, which you can contact at 866-447-7559. If you have other questions, please feel free to contact us at 580-772-5574.

If you have any questions or think you are a victim of identity theft please contact one of our associates at (580) 772-5575, and together, with our present safeguards and continuing diligence and your awareness, we can meet the challenge of keeping your financial identity private and secure.

Thank you.

