Protect yourself from Fraud and Identity Theft

According to the Federal Trade Commission here are some actions to take to help protect yourself after a data breach:

- Check your credit reports. A credit report includes information on where you live, how you pay your bills, and whether you've been sued or have filed for bankruptcy. Nationwide credit reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home. Obtain copies of your credit reports from Equifax, Experian, and TransUnion by visiting **AnnualCreditReport.com**, calling 1-877-322-8228, or writing them at: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The Fair Credit Reporting Act (FCRA) requires each of the nationwide credit reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months. Accounts or activity that you don't recognize could indicate identity theft. Visit **IdentityTheft.gov** to find out what to do.

- Consider placing a credit freeze on your files. This tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your file, they may not extend the credit. Fees vary, from free to $10, typically. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts. To place credit freezes these are the contact numbers:
  - TransUnion - 1-888-909-8872
  - Experian - 1-888-397-3742
  - Equifax - 1-800-349-9960

- 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. Three national credit reporting companies keep records of your credit history. If someone has misused your personal or financial information, call **one** of the companies and ask for an initial fraud alert on your credit report. If you're concerned about identity theft, but haven't yet become a victim, you can also place an initial fraud alert. For example, you may want to place a fraud alert if your wallet, Social Security card, or other personal, financial or account information are lost or stolen. You may also want to place a fraud alert if your personal information was exposed in a data breach. A fraud alert is free. The company you call must tell the other companies about your alert. Here are contact numbers for placing a fraud alert:
  - TransUnion - 1-800-680-7289
  - Experian - 1-888-397-3742
  - Equifax - 1-800-525-6285

  An initial fraud alert can make it harder for an identity thief to open more accounts in your name. When you have an alert on your report, a business must verify your identity before it issues credit, so it may try

to contact you. The initial alert stays on your report for at least 90 days. You can renew it after 90 days. Be sure the credit reporting companies have your current contact information so they can get in touch with you.

- 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.

- Protect your debit card with smsGuardian. smsGuardian is an anti-fraud notification service that sends text alerts directly to your mobile phone or other SMS-enabled device. When certain debit card transactions take place, this added layer of security alerts you to possible fraudulent use of your card. If you receive a text about a transaction you think is fraudulent, you can reply immediately and your card will be blocked from further activity. The text alert will also describe how to respond in order to stop the current transaction right from your mobile device. For more information, visit **www.amnat.com/personal/smsguardian**.

- For more information about these and other privacy, identity and online security topics, visit the Federal Trade Commission's website at **www.consumer.ftc.gov/topics/privacy-identity-online-security**.

  For more targeted topics:

  Equifax Data Breach: What to Do
  www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

  Free Credit Reports
  www.consumer.ftc.gov/articles/0155-free-credit-reports

  How to Keep Your Personal Information Secure
  www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

  Place a Fraud Alert
  www.consumer.ftc.gov/articles/0275-place-fraud-alert