Knowledge is Key

Reduce Your Risk of Identity Theft

4 Easy Steps to Protect Your Personal Information

1. Know who you share information with.
2. Store and dispose of your personal information securely, especially your Social Security number.
3. Ask questions before deciding to share your personal information.
4. Maintain appropriate security on your computers and other electronic devices.

Additional Proactive Steps You Can Take

1. Check your bank accounts daily (including checking, savings, and credit card statements).
2. Do not use the same security questions/answers and login credentials for accounts. Financial account credentials should be different from those used for social media, utilities, etc. Each account owner should have a separate login from other owners. Never share login credentials for the same account.
3. Select security questions only you know the answer to. Many security questions ask for answers that may be available in public records or online, like your zip code, mother's maiden name, and birthplace. That is information a motivated attacker can obtain. Don't use questions with a limited number of responses that attackers can easily guess — like the color of your first car.
4. Choose a strong password that is a mix of upper- and lower-case letters, numbers and special characters (i.e. ! love 2 go biking). Avoid using any words or phrases that contain your name, initials or birthdate. Weak passwords are a significant cause of identity theft, email compromise and financial loss. Test the strength of your password at: https://www.howsecureismypassword.net/.
5. Know that the bank will never contact you and ask for your full debit card number or 3-digit security code on the back of your card. Should you receive any calls requesting this information, hang up the phone and contact the bank immediately at 1-877-888-5629.
6. Never provide your Social Security number to anyone unless you have initiated the request. Likewise, never share your full card number and 3-digit code on the back of your card.

Examples of

How Your Information Could Be Compromised

1. Your email account is compromised.
2. An outside party obtains access to your online banking.
3. A non-First Mid online system is compromised.
4. Fraudulent access takes place on your First Mid or other debit/credit card accounts.
5. Unauthorized requests for credit occur on your credit report.

If Your Personal Information Has Been Compromised

1. Stay alert; monitor your credit card and bank accounts closely.
2. It's important to immediately change your online login information, passwords, and security Q&A for the account(s) that were affected, along with your other online accounts if they have similar passwords and security Q&A, to limit the reach of the hackers' arms.
3. Obtain a 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.

   Additional information on your free credit report can be found at: https://www.consumer.ftc.gov/articles/0155-free-credit-reports.