About Fraud

Identity Theft - Identity theft, when someone uses your personal information with your permission, happens all the time. According to a 2012 report from the Bureau of Justice, 7% of households throughout the country experienced identity theft. That means if there are 15 houses on your street, at least one has experienced identity theft. Javelin Strategy and Research reported there were more than 12.6 million individual victims and $21 billion lost in 2012. Victims lose an average of $2,200, according to the Bureau of Justice. The Federal Trade Commission reported in 2013 that identity theft was the top consumers complaint for the 13th year in a row. If you haven't been a victim, odds are someone you know has been touched. Here are some of the most widespread:

Credit Card Fraud - Credit cards are opened in a victim's name or unauthorized charges are made to an existing card.

Unauthorized Phone Services - New mobile phone service is established in a victim's name.

Bank Fraud - A new bank account is opened in a victim's name, fraudulent checks are written or unauthorized withdrawals are made from an account.

Fraudulent Loans - Personal, business, auto or real estate loans are obtained in a victim's name.

Government Documents or Benefits - Access is gained to a victim's government documents, such as his/her driver's license or Social Security Number; a tax return is filed fraudulently or government benefits are obtained through fraudulent means.

How does it happen? Traditionally, criminals gained access to a victim's personal information from a stolen wallet or mail. Today, online and mobile threats continue to grow. With the access to social media sites, more information can be available. Criminals use many means to access this information, including exploiting software vulnerabilities, launching phising attacks, accessing electronic payment options and using any means possible to access personal information.

How does Merchants Bank protect me? Merchants Bank uses a combination of safeguards to protect your information including: employee training, encryption of information, and fraud detection programs.

Identity Theft Prevention Tips

1. Always lock your vehicle.
2. Put private information away when others will be in your home, such as cleaning people, repair people, babysitters, and others.
3. Don't leave private information on your work desk.
4. Use online or mobile banking to monitor accounts regularly.
5. Do not keep large balances in checking accounts that have checks or a debit card connected to them. Transfer excess funds to a savings account instead.
6. If you are not going to use checks, do not order any.
7. Do not provide your Social Security number or personal credit information to anyone over the phone or online unless you are the one who initiated the call and are familiar with the business.
8. Shred all financial statements, credit card offers, and any unused cards before recycling them.
9. Protect your bank and credit card Personal Identification Numbers (PINs) and other passwords by changing them frequently, using a combination of letters and numbers when possible, and not sharing them with others.
10. Keep a list of your credit cards, account numbers, expiration dates, and customer service or fraud department telephone numbers in a secure place away from the cards for easy access.
11. Never keep your Social Security Card in your wallet.
12. Carefully check through your credit card and bank activity regularly online, as well as your monthly statements and immediately report unusual activity.
13. Be cautious when entering a login ID and PIN for all online account access, especially when on a public network. Make sure you are on a secure website.
14. Set up text or email alerts from your bank for certain transactions, such as transactions over $500. Alerts are available through the "Manage My Money" function in Merchants Online Banking.
15. Sign up for eStatements to reduce the likelihood of paper statements being stolen.
16. Make sure the virus protection software on your computer is up to date.
17. Use the passcode feature on your smart phone and other mobile devices. It will be more difficult for people to access your personal information in the event it is lost or stolen.
18. Social media sites may capture your personal information and makes it available, making it more accessible to criminals. Be careful what you post on social media websites. Criminals can use information as such as birthdays, high schools, colleges, pet names

Getting a Child's Credit Report

One in 40 households with children under the age of 18 had at least one child whose personal information had been compromised, according to a 2012 study by Javelin Strategy and Research. Children can get their credit reports from the agencies listed below. Children under 13 should have their parent or legal guardian request the information. Information about the child needed for a written request may include: legal name, address, birth date, a copy of the child's birth certificate, and a copy of the child's social security card. You will also need to provide documentation identifying yourself as a parent or legal guardian.

Credit Reporting Agencies

If you believe you've been a victim of identity theft, you can report it to these Credit Reporting Agencies:

Equifax	www.equifax.com	To report fraud, call: 1-800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241
Experian	www.experian.com	To report fraud, call: 1-888-EXPERIAN (397-3742) and write: P.O. Box 9532, Allen, TX 75013
Trans Union	www.tuc.com	To report fraud, call: 1-800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834

Let the FTC Know

If you've been a victim of identity theft, file your complaint with the Federal Trade Commission:

Identity Theft Hotline Toll-Free 1-877-438-4338
TDD 202-326-2502
By mail: Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue
Washington, DC 20580
Online www.consumer.gov/idtheft

Merchants Bank

The Bank that Service Built