



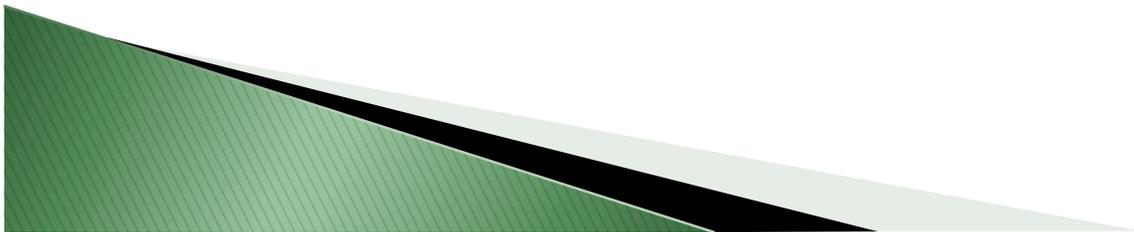
Identity Theft

Protecting Your Identity and Safeguarding
your Financial Information



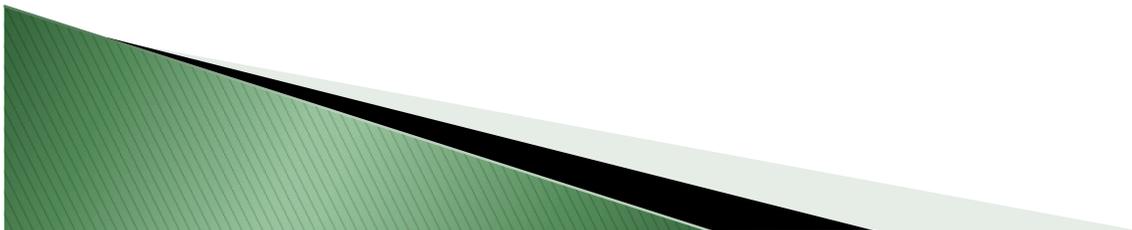
Overview

- ▶ What identity theft is and how it occurs
- ▶ How to spot identity theft
- ▶ How to protect yourself
- ▶ What to do if you're a victim of identity theft
- ▶ What's next



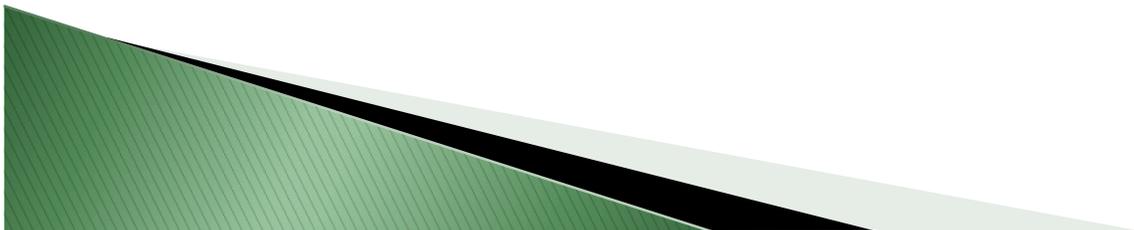
What is Identity Theft?

- ▶ Fraud, attempted or actual, using identifying personal information without authority. Once personal information is obtained criminals may attempt to:
 - Open fraudulent credit cards in your name;
 - Add authorized users to existing credit cards;
 - Apply for fraudulent mortgages or loans in your name;
 - Open fraudulent consumer or banking accounts in your name.



Identifying Information

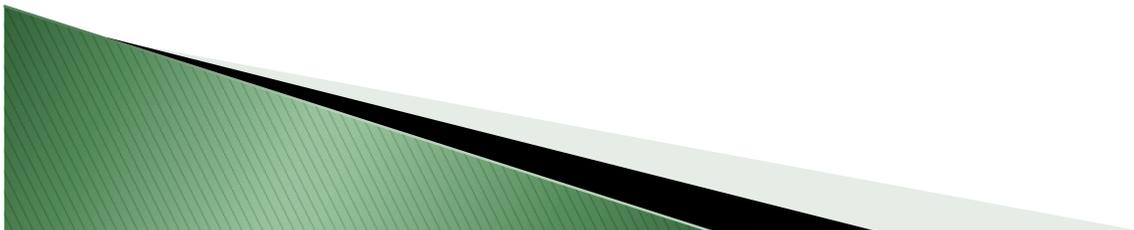
- ▶ The Federal Trade Commission defines “identifying information” as,
“...any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any of the following:”
 - Name;
 - Social Security Number;
 - Date of Birth;
 - Official state or government issued licenses;
 - Taxpayer identification number;
 - Credit or debit card numbers.



How Identity Theft Occurs

Identity thieves may attempt to:

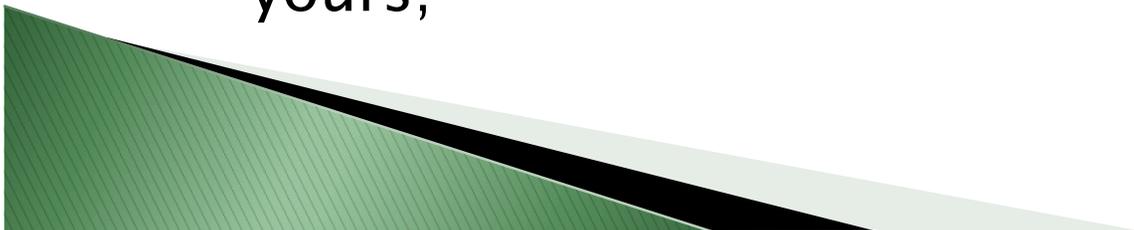
- “Dumpster Dive”;
- Steal mail or attempt to make address changes for your mail;
- Steal wallets or purses;
- Send “phishing” or fake emails in an attempt to get personal information or account credentials;
- Attempt “Social Engineering”, or manipulate you into doing something you normally wouldn’t.



The Red Flags of Identity Theft

Red flags are warning signs that you or someone you know may be a victim of identity theft. Red flags include:

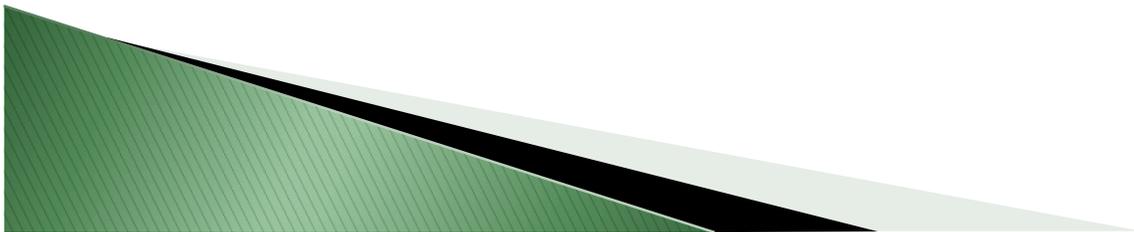
- You lose a wallet or purse containing confidential identifying information;
- You receive credit cards you didn't apply for;
- Your bills or financial statements don't arrive;
- You are turned down or offered unfavorable credit terms for no reason;
- Your credit report shows accounts that are not yours;



Protecting Your Personal Information

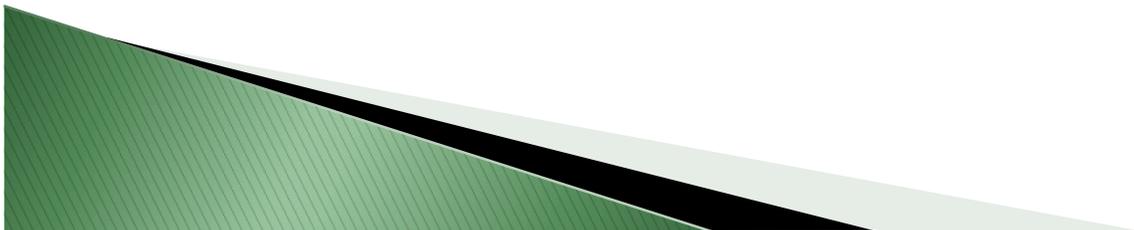
The best way to avoid becoming a victim of identity theft is to proactively protect your personal information:

- Avoid carrying Social Security cards, Passports, or birth certificates;
- Review all bills and statements often and report any suspicious activity;
- Secure or shred bills and statements;



Protecting Your Personal Information cont.

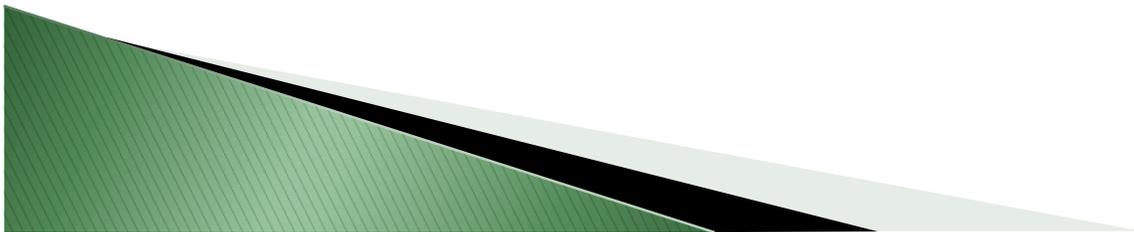
- Sign up for your free e-statements from St. Anne's to receive your financial statements electronically;
- Maintain and monitor your St. Anne's accounts with free Online Banking and Billpay;
- Review your credit report at least annually;
- Only use secure mail boxes when mailing material containing confidential information.



Identity Theft Online

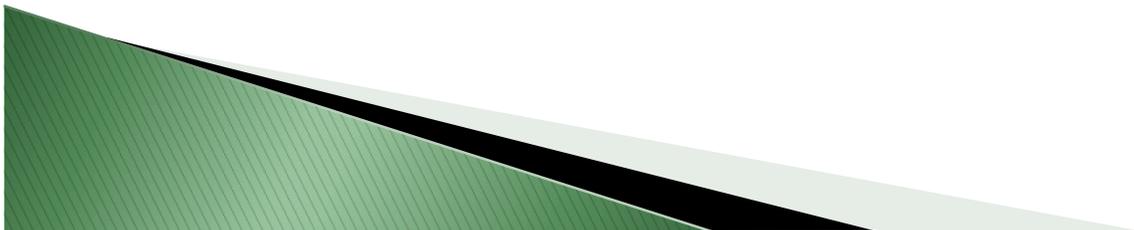
The internet provides convenience for everyday activities like shopping and banking, it can also be very risky.

- ▶ About 30% of home computers in the US are infected with a virus.
- ▶ Many viruses target account credentials or capture Social Security numbers or credit/debit card numbers.



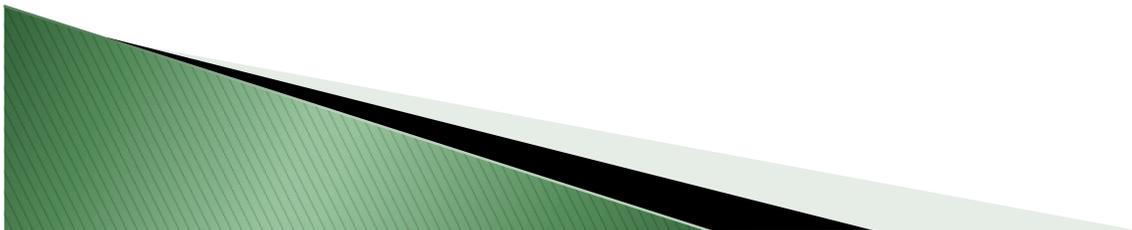
Protecting Yourself Online

- ▶ Avoid risky online behavior;
- ▶ Be sure all your devices are running active, current, and up-to-date anti-virus protection;
- ▶ Avoid opening unsolicited emails or accessing attached links;
- ▶ When shopping online try to use a credit card with a low credit limit;
- ▶ Try to use strong passwords for online accounts;
- ▶ Avoid using the same password for multiple sites;
- ▶ If possible use a separate “clean” device for all online shopping and account activity.



How St. Anne's Protects You

- ▶ St. Anne's is committed to protecting your information.
 - Verification of ID's prior to opening new accounts or transacting business.
 - Identification scanning to assist in ID verification.
 - Member's can request to add alerts to their accounts in the case of fraudulent activity.
 - St. Anne's will never call you requesting that you provide personal information.
 - Keeping your contact information current with St. Anne's to assist if there is any fraudulent activity.



How to Respond If you are a Victim of Identity Theft

If you believe you are a victim of identity theft take the following steps:

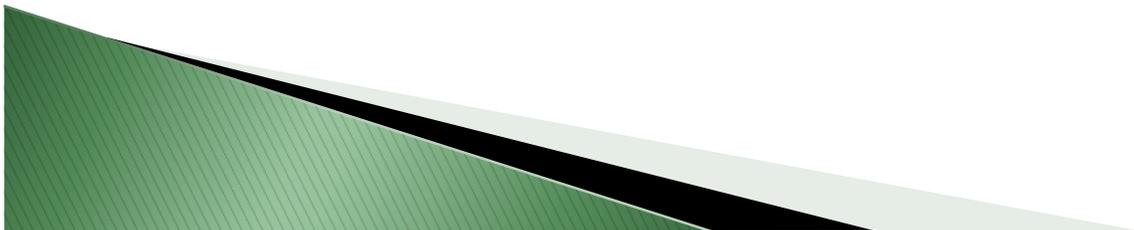
- Don't panic, stay calm, and document everything;
- Contact the three credit bureaus and place fraud alerts;
 - Equifax
 - Experian
 - TransUnion
- Verify that all suspicious activity is fraudulent;
- Contact companies that fraudulent activity has occurred and close all suspicious accounts;
- File a police report;
- Contact the Federal Trade Commission.



What's Next: Removing Fraudulent Charges

After you have reported the identity theft you will have to work with the companies in which fraudulent activity has occurred.

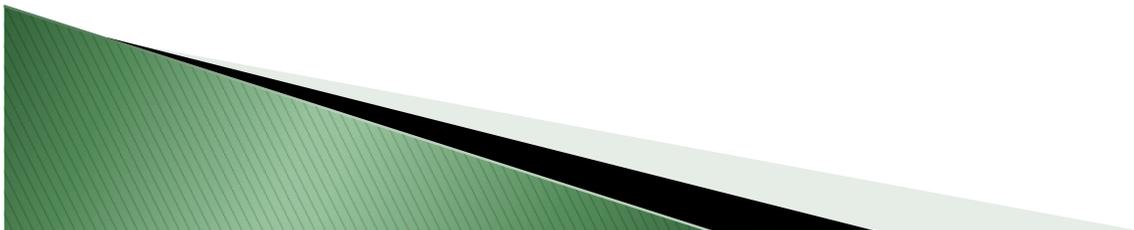
- Explain the situation and report to them all fraudulent charges and ask that they be removed;
- Document who you speak with;
- Request a letter of confirmation of removed charges.



What's Next: Cleaning Your Credit

Write to each of the three credit bureaus to remove fraudulent information from your credit report. Provide the credit bureau with the following information:

- Copy of your FTC Identity Theft Report and proof of your identity
- Provide them which information on your report was from identity theft
- Retain any and all communication between yourself and the credit bureaus

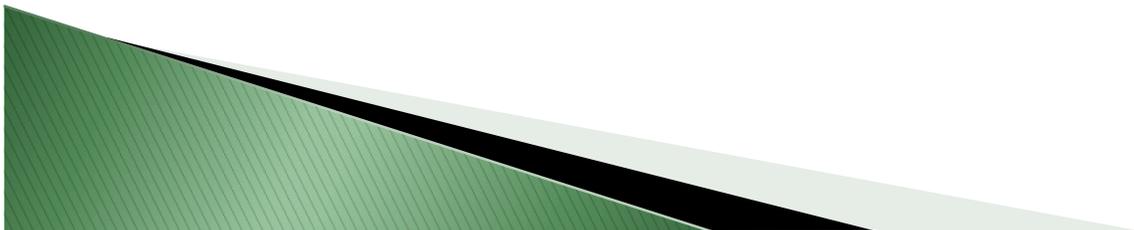


Extending Fraud Alerts or Credit Freeze

Victims of identity theft can contact the three credit bureaus to request an extended fraud alert or credit freeze.

Extended Fraud Alerts – Allows consumer to access their credit report as long as the company takes steps to verify the consumers identity.

Credit Freeze – Allows consumer to stop all access to their credit report unless it is lifted or removed. Fees may be associated for placing, lifting, or removing the credit freeze.



Resources

Credit Bureaus

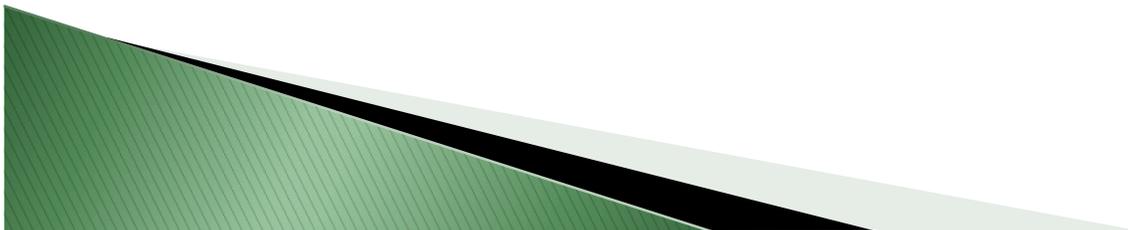
▶ **Equifax** – Equifax Consumer Fraud Division P.O. Box 740256, Atlanta, GA 30348-5069 (1-888-766-0008) www.equifax.com

▶ **Experian** – P.O. Box 9532, Allen, TX 75013; (1-888-397-3742); www.experian.com

▶ **TransUnion** – Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634-6970; (1-800-680-7289); www.transunion.com

Federal Trade Commission (FTC)

Consumer Protection and Information – www.consumer.ftc.gov
www.identitytheft.gov



Additional Information

- ▶ Like St. Anne's on Facebook to receive news and alerts on the Credit Union or Scams affecting our community.
- ▶ Visit www.Stannes.com to enroll in Online Banking and e-Statements.
- ▶ Visit or call your local branch if you have questions about your account.

