Equifax: 1-800-525-6285
www.equifax.com
P.O. Box 740241
Atlanta GA. 30374-0241

Experian:1-888-EXPERIAN (397-3742)
www.experian.com
P.O. Box 9532
Allen, TX 75013

Trans Union: 1-800-680-7289
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

Report fraud with unknown suspect.
www.ftc.gov

Online fraud with known suspect or business.
www.ic3.gov

Identity theft resources
www.idtheftcenter.org
www.lookstoogoodtobetrue.com

If you suspect your checks are being forged, and want to put an alert on your checking account call:
Telecheck 1-800-710-9898 or
Certegy 1-800-437-5120

If you suspect your checking account information is being used to pass forged checks contact:
SCAN 1-800-262-7771

Credit Report
www.annualcrditreport.com

IDENTITY THEFT/FRAUD INITIAL STEPS

HOW TO PROTECT YOURSELF

INVER GROVE HEIGHTS
POLICE DEPARTMENT

8150 BARBABA AVE
INVER GROVE HEIGHTS
MN 55077

DISPATCH: 9-1-1
OFFICE: 651-450-2525
FAX: 651-450-2543
www.ci.inver-grove-heights.mn.us

COMPONENTS OF IDENTITY

WHAT IS IDENTITY THEFT?

Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes.

PERSONAL INFORMATION

Despite a persons best efforts to manage the flow of their personal information, skilled identity thieves may use a variety of methods to gain access to the information. The following is how personal information is obtained;

- Steal wallets and/or purses left in vehicles or unattended carts at local businesses
- Obtain information from businesses or other institutions by stealing records or information while they're on the job or bribing an employee who has access to these records
- Steal mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- Rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."
- They may steal personal information they find in your home.
- They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or "pretexting" by phone.

INITIAL STEPS: FOR IDENTITY THEFT VICTIMS

1. Close the account(s) that you know, or believe, have been tampered with or opened fraudulently.
   - If fraudulent charges and or debits are on existing accounts, ask the representative to send you the company's fraud dispute forms.
2. Place a fraud alert on your credit report and review your credit report(s).
   - Fraud alerts can help prevent an identity thief from opening any more accounts in your name.
   - Contact the toll-free fraud number of any of the three consumer reporting companies (located on the back page) to place a fraud alert on your credit report.
   - You will only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports.
3. Contact your local law enforcement agency and file a police report
   - It can help you deal with creditors who need proof of the crime.
   - If you are a victim of fraud such as; check forgery or credit card fraud and it is related to your identity theft and the crime happened in another city, contact the corresponding local law enforcement agency to report it.

YOU SHOULD ALWAYS KEEP A LIST OF YOUR CREDIT CARD AND BANK ACCOUNT NUMBERS IN A SAFE PLACE, IN CASE YOU NEED TO CANCEL THE ACCOUNTS.

WHAT YOU CAN DO TO REDUCE RISK OF IDENTITY THEFT

- Never reveal personal information without knowing why it is needed.
- Never carry your social security card with you, secure it in a safe place.
- Place passwords on your credit card, bank, and phone accounts.
- Secure personal information in your home, shred unnecessary bills, credit card offers, etc…
- Be vigilant about reviewing credit card and bank statements for any unauthorized transactions.
- Never use your personal mailbox for outgoing bills, the flag is a sign to thieves that personal information might be inside.
- Have the Post Office hold your mail if away on vacation.
- **Never** leave purses or wallets in your motor vehicle.
- Take precaution when using your PIN at the ATM or other locations so no one is able to view your input.
- Have your name removed from credit card offers, and lists of direct mailings offering credit or services.

FRAUD

Fraud is a multi-million dollar a year problem. The use of the internet has made fraud global; the following are some examples of different crimes that occur:

- Online Auction Fraud
- Online Credit Card Fraud
- Employment/Business Opportunities
- Identity Theft
- Investment Fraud
- Lotteries
- Nigerian Money Scam or "419"
- Phishing/Spoofing
- Reshipping
- Third Party Receiver of Funds

ONLINE AUCTION FRAUD

- Before you bid, contact the seller with any questions you have.
- Review the seller's feedback.
- Be cautious when dealing with individuals outside of your own country.
- Ensure you understand refund, return, and warranty policies.
- Determine the shipping charges before you buy.
- Be wary if the seller only accepts wire transfers or cash.
- If an escrow service is used, ensure it is legitimate.
- Consider insuring your item.
- Be cautious of unsolicited offers.

ONLINE CREDIT CARD FRAUD

- Ensure a site is secure and reputable before providing your credit card number online.
- Don't trust a site just because it claims to be secure.
- If purchasing merchandise, ensure it is from a reputable source.
- Promptly reconcile credit card statements to avoid unauthorized charges.
- Do your research to ensure legitimacy of the individual or company.
- Beware of providing credit card information when requested through unsolicited emails.

EMPLOYMENT/BUSINESS OPPORTUNITIES

- Be wary of inflated claims of product effectiveness.
- Be cautious of exaggerated claims of possible earnings or profits.
- Beware when money is required up front for instructions or products.
- Be leery when the job posting claims "no experience necessary".
- Do your research to ensure legitimacy of the individual or company.
- Be cautious when dealing with individuals outside of your own country.
- Be wary when replying to unsolicited phone calls or emails for work-at-home employment.
- Research the company to ensure they are authentic.
- Contact the Better Business Bureau to determine the legitimacy of the company.

INTERNET ESCROW SERVICES FRAUD

- Always type in the website address yourself rather than clicking on a link provided.
- A legitimate website will be unique and will not duplicate the work of other companies.
- Be leery of escrow sites that only accept wire transfers or e-currency.
- Be watchful of spelling errors, grammar problems, or inconsistent information.

Beware of sites that have escrow fees that are unreasonably low.

INVESTMENT FRAUD

- If the "opportunity" appears too good to be true, it probably is.
- Beware of promises to make fast profits.
- Do not invest in anything unless you understand the deal.
- Don't assume a company is legitimate based on "appearance" of the website.
- Be leery when responding to investment offers received through unsolicited mail or email.
- Be wary of investments that offer high returns at little or no risk.
- Independently verify the terms of any investment that you intend to make.
- Research the parties involved and the nature of the investment.
- Be cautious when dealing with individuals outside of your own country.
- Contact the Better Business Bureau to determine the legitimacy of the company.

LOTTERIES

- If the lottery winnings appear too good to be true, they probably are.
- Be cautious when dealing with individuals outside of your own country.
- Be leery if you do not remember entering a lottery or contest.
- Be cautious if you receive a telephone call, mail or emails stating you are the winner in a lottery.
- Beware of lotteries that charge a fee prior to delivery of your prize.
- Be wary of demands to send additional money to be eligible for future winnings.
- It is a violation of federal law to play a foreign lottery via mail or phone.

NIGERIAN MONEY SCAM OR "419"

- If the "opportunity" appears too good to be true, it probably is.
- Do not reply to mail or emails asking for personal banking information.
- Be wary of individuals representing themselves as foreign government officials.
- Be cautious when dealing with individuals.
- Be cautious when dealing with individuals outside of your own country.
- Beware when asked to assist in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.

PHISHING/PRETEXTING

- Be suspicious of any unsolicited email or phone calls requesting personal information.
- Avoid filling out forms in email messages that ask for personal information.
- Avoid giving out personal information over the phone.
- Always compare the link in the email to the link that you are actually directed to.
- Log on to the official website instead of "linking" to it from an unsolicited email.
- Contact the actual business that supposedly sent the email to verify if the email is genuine.

RESHIPPING

- Be cautious if you are asked to ship packages to an "overseas home office."
- Be cautious when dealing with individuals outside of your own country.
- Be leery if the individual states that his country will not allow direct business shipments from the United States.
- Be wary if the "ship to" address is yours but the name on the package is not.
- Don't accept packages that you didn't order.
- If you receive packages that you didn't order, either refuse them upon delivery or contact the company where the package is from.

THIRD PARTY RECEIVER OF FUNDS

- Do not agree to accept and wire payments for auctions that you did not post.
- Be leery if the individual states that his country makes receiving these type of funds difficult.
- Be cautious when the job posting claims "no experience necessary".
- Be cautious when dealing with individuals outside of your own country.

WHAT TO DO IF YOU BECOME A VICTIM

- Close the account(s) that you know, or believe, have been tampered with or opened fraudulently.
- Place a fraud alert on your account.
- Contact the toll-free fraud number of any of the three consumer reporting companies (located on the back page) to place a fraud alert on your credit report. (You only need to contact one of the three companies)
- Collect all documentation and report the crime to your local Law Enforcement Agency.