Identity Theft Assistance:
Safeguarding Your Identity

WHEN DOES IDENTITY THEFT OCCUR?

Identity theft occurs when someone uses your name or personal information, such as:

- Your social security number;
- Driver's license number;
- Credit card number;
- Telephone number;
- Or other account numbers.

...*WITHOUT YOUR PERMISSION!!*

With minimal information identity thieves can open credit accounts, bank accounts, telephone service accounts, and make major purchases - all in your name. Information can be used to take over your existing accounts, or to open new accounts.

Identity Theft can take countless hours to resolve and can result in damage to your credit rating, denials of credit and complicate job offers. The sooner you find out about an identity theft situation, the sooner you can recover your personal information, so it is good to know how to keep yourself protected.

HOW DOES IDENTITY THEFT HAPPEN?

Identity theft commonly begins with the **loss or theft of a wallet or purse**. But there are many other ways that criminals can get and use your personal information in order to commit identity theft. The following are some examples:

*One evening, you sit down to pay your monthly bills. You write the checks, toss the statements in the trash and put the container out on the curb for the morning's trash pick-up. While you sleep, **"dumpster divers**" go through your trash looking for papers you've thrown away. They discover a gold mine of information that can be used for fraudulent purposes – your name, address, phone number, utility service account numbers, credit card numbers, and your social security number.*

or

You receive an e-mail message from what appears to be your Internet Service Provider (ISP). The message requests that you update the information they have on file about you – your name, credit card number, bank account number, etc. – by replying to the e-mail or going to a specific Web site address to provide the information. However, neither the message nor the Web site address is from your ISP. They belong to someone who wants to get your information to steal your identity. This is sometimes known as 'phishing'.

In addition, thieves can steal information in the following ways:

- Mail stolen from a mailbox;
- Change of address forms redirecting the destination of your mail;
- Home computers infected with viruses that transmit data to thieves;
- A perpetrator gains access to a place that keeps records for many people;
- The perpetrator contacts a person through the mail, telephone, or e-mail, and attempts to get information, usually by asking to 'verify' some data;
- Roommates, hired help, and landlords all have access to a person's home, and it is possible for them to access private information.

The perpetrator then uses the information to apply for loans, credit cards, etc. The perpetrator then charges large amounts to the credit cards or defaults on the loans, all under the victim's name.

HOW COMMON IS IDENTITY THEFT?

- It is one of the fastest growing crimes.
- It is the top consumer fraud complaint.
- There are between 500,000-750,000 victims per year.

WHAT CAN YOU DO TO PROTECT YOURSELF FROM IDENTITY THEFT?

Although identity theft is on the rise, there are a number of steps you may take to help minimize the risk of it happening to you.

Be Aware. Monitor your financial statements regularly.

Obtain your credit reports from each of the three major credit bureaus once every 6-12 months. Review these reports for any inaccurate information, or any transactions that you were not aware of or did not authorize.

Secure your personal information at home. Consider keeping your sensitive, personal information in a safe or other location accessible only by you.

Ask about security measures in your workplace. Find out who can obtain your personal information through work, how your information is secured, and how they discard personal records. Keep your purse or wallet in a safe place at work.

Avoid giving out personal information over the phone. Especially when the telephone call is initiated by another party. Identity thieves may pose as a representative of a legitimate organization with whom you do business and may contact you to "verify" your information.

Be suspicious of providing personal information online. Identity thieves use a practice called 'phishing' where they send emails that claim to be from a legitimate source – such as a bank, government entity or your ISP – and ask you to update your account or personal information. Verify unsolicited email by calling the financial institution or government agency directly, or through a new Internet session.

Carry only the information you need. Only take with you the credit cards you need, and avoid carrying your Social Security card.

Regularly review your recent Card account activity. Accessing your account online is a great way to stay up-to-date on recent charges. To learn more about managing your American Express Card account online, visit www.americanexpress.com/mycardaccount. Also, American Express can notify you immediately of irregular account activity if you sign up to receive Alerts. For more information on Alerts, visit www.americanexpress.com/alerts.

Shred documents containing your personal information before disposing. Identity thieves have been known to "dumpster dive" to obtain documents with personal information that have been discarded. You may obtain a paper shredder at any local office supply company.

Have the Postal Service hold your mail if you are going to be gone for a few days or more. Since identity thieves have also been known to obtain personal information by collecting individual's mail before they return home, it is a good idea to collect your mail as soon as possible and to have the Postal Service hold your mail at the post office if you are planning on being away for any period of time. Another way to prevent account information from being stolen in the mail or from the trash is to reduce the amount of paper with account references. You can find out more about alternate delivery options for your statement information at www.americanexpress.com/onlinestatement.

HOW CAN YOU PROTECT YOUR PERSONAL COMPUTER FROM IDENTITY THEFT?

Many of us store financial records, tax information, birth dates, social security numbers and passwords on our personal computers. Follow these tips to help keep your personal information safe.

- Ensure your virus protection software is up to date.
- Do not download files, launch attachments, or click on hyperlinks from people you don't know. You could be exposing your system to a virus.
- Use a firewall program to help prevent unauthorized people from accessing your computer.
- Always use a secure browser to protect the security of your online transactions.

HOW CAN I TELL IF I AM A VICTIM OF IDENTITY THEFT?

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

- Failing to receive bills or mail when expected could mean an address change by the identity thief;
- Receiving credit cards for which you did not apply;
- Denial of credit for no apparent reason; or
- Receiving calls from debt collectors or companies about merchandise or services you didn't buy.

Order a copy of your credit report from any of the three major credit bureaus. If at this time you feel you may be a victim, you should initiate a fraud alert. Once you receive your report, review it for accuracy. If you find inaccurate information, check your reports from the other two credit bureaus. Of course some inaccuracies could be because of clerical, computer, or other errors and may not be a result of identity theft. It may take 7-10 business days to receive your reports.

Equifax

Order Credit Report: 1.800.685.1111

Report Fraud: 1.800.525.6285

www.equifax.com

Experian®

Order Credit Report: 1.888.397.3742

Report Fraud: 1.888.397.3742

www.experian.com

TransUnion℠

Order Credit Report: 1.800.888.4213

Report Fraud: 1.800.680.7289

www.tuc.com

Tips for How to Read Your Credit Report

- Check to make sure you recognize all accounts listed in your report and that the balances are in line with your records.
- Check the section listing the persons and entities that have requested or received a copy of your report. If you do not recognize a person or entity, you may want to further inquire.
- Make sure there were no inquiries to your credit report for loans or accounts you did not apply for. If there are accounts you do not recognize, this may be a sign that an identity perpetrator has fraudulently opened an account in your name.
- Check the address section to confirm there are no addresses listed for places you have never lived. If there are addresses you do not recognize, this may be a sign that an identity perpetrator has redirected your mail.
- Make sure your Social Security number is listed correctly.
- Make sure the employment history lists accurate information.
- Make sure the information is consistent across the 3 credit bureaus.
- If you identify any incorrect or suspect information, contact the credit bureau immediately. If the incorrect or suspect information is linked to a particular creditor, you will want to contact that creditor as well.

REMEMBER:

Act fast! Any protections you have are stronger if you act quickly to try to correct potential identity theft.