IF YOU ARE AN IDENTITY THEFT VICTIM

If you spot identity theft early and act quickly, you can minimize damage. Take the following steps:

Keep a journal. Record all actions you take to clear your name. Include names of agencies, businesses, and individuals. Keep detailed records of phone calls and copies of correspondence.

File an Identity Theft Affidavit. Contact the Federal Trade Commission at (877) 438-4338, or visit www.ftc.gov to file a complaint and create an Identity Theft Affidavit. Your police report combined with your Affidavit will serve as the **Identity Theft Report** you will use to dispute fraudulent accounts.

File a police report. Visit your local precinct and give the officer taking the report a copy of your FTC Identity Theft Affidavit and any other proof of theft. Make sure the police report lists all fraudulent reports. Keep the officer's contact information. Get your complaint number and a copy of your police report. You may need the police report to prove that you are a victim when disputing fraudulent charges or accounts.

Dispute fraudulent information on your credit report. Send your Identity Theft Report to each credit reporting agency with a letter requesting that fraudulent accounts be blocked from showing up on your credit report. (Continue to monitor your credit reports afterwards, in case fraudulent information is placed back on your reports.)

Contact your creditors. It's a good idea to notify your creditors both by phone and in writing by certified mail that you are a victim. Include a copy of your Identity Theft Report. Request that they stop reporting fraudulent information to the credit reporting agencies.

Contact your bank. Report lost, stolen or forged checks and lost or stolen deposit tickets and bank statements, to your bank. If your bank account or a credit line has been compromised in any way even if you believe the compromise is insignificant, notify the bank, close the account completely, and open a new account or credit line. Report lost or stolen debit cards. Take action quickly to limit your liability.

Contact the DMV. If your driver's license is stolen, take your police report to your local DMV when you ask for a replacement license. Ask them to attach a copy of the report to your records. If you have evidence that another person was issued a license, registration or title certificate in your name, file a form FI–17 (Report of Unauthorized use of License/ Registration). You may need to change your license number if the thief is using it.

Contact Utilities. Notify your utility and telephone companies that you've been victimized. An identity thief may attempt to open a new account in your name using a utility bill as proof of residence.

Contact the Social Security Administration. If you suspect that somebody is using your Social Security number, call the Social Security Administration fraud hotline at (800) 269-0271 or visit www.ssa.gov/oig. You can check your earnings record by calling (800) 772-1213.

Change/Add Passwords. To be safe, change all account passwords. If an account does not have a password, add one if possible. Use strong passwords, at least 8 characters long that include a mix of symbols, numbers, and lower and uppercase letters. Don't use words found in the dictionary, common alphabetical, numerical or keyboard sequences, or any part of your Social Security number or personal information as a password.

USE A FRAUD ALERT AND SECURITY FREEZE

If you are a victim or think you may be a victim of ID theft, consider placing a "security freeze" or "fraud alert" in your file at the three major credit reporting agencies (Equifax, TransUnion, and Experian).

A **security freeze** generally stops creditors from accessing your credit files to review your credit history, thus preventing any new lines of credit from being opened for you, unless you authorize the agencies to allow access. The procedures for obtaining a security freeze are slightly different for each of the three credit reporting agencies, and you must place one with each of the three agencies. Visit their websites (www.equifax.com, www.transunion.com, www.experian.com) to find out how.

A **fraud alert** alerts creditors to contact you before they open new accounts or change existing accounts. Unlike a security freeze, a fraud alert does not lock down your credit; while creditors will get an alert message, there is no guarantee they will not issue credit. A fraud alert generally lasts for 90 days, though it can be extended. To obtain a fraud alert, ask one of the three credit reporting companies to put an alert on your credit report. That agency is required to tell the other two agencies, but you should confirm with the company you call that it will call the other two. Visit the Equifax, TransUnion, or Experian website to find out how to place an alert.

GET HELP

For more information or to file a complaint, visit our website at **www.dfs.ny.gov** or callus at **(800) 342-3736**.

What You Need to Know About...

IDENTITY THEFT

This guide is provided for informational purposes only and does not constitute legal advice.

www.dfs.ny.gov
(800) 342-3736

To have a DFS outreach professional present a program on identity theft to your organization, contact James Dees at 212-480-7246.

Important information about protecting yourself and your personal information and what to do if you are a victim.

WHAT IS IDENTITY THEFT?

Identity theft is the practice of stealing someone's identifying personal information with the intent to use it to fraudulently obtain goods, benefits, or services. It can occur online or offline. New York has one of the highest per capita rates of identity theft in the country. Identity theft can result in damaged credit, denial of employment, credit, and insurance, and professional licenses. Victims often spend a significant amount of time and money reclaiming their good name and reputation.

TIPS TO PROTECT YOURSELF

You are the first line of defense in protecting yourself from identity thieves. Here are some measures you can take to prevent your personal information from being stolen:

Check Your Credit Report. Checking your credit reports on a regular basis is a good way to spot identity theft early on. If an identity thief is opening new accounts in your name, these accounts are likely to show up on your report. New Yorkers may obtain a free credit report from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) once a year. Visit www.annualcreditreport.com or call 877-322-8228 to obtain these free reports. Take advantage of this by ordering a report from a different agency every four months, and check it carefully for accounts you did not open and other questionable activity.

Store and Dispose of Sensitive Information Securely. Keep your Social Security card, birth certificate, and other important identification and financial documents in a secure place. Be cautious about where you leave sensitive material like bills and bank statements, and digital devices that may contain sensitive material or personally identifying information. Before discarding mail, it is advisable to shred sensitive documents. Report lost or stolen credit, debit, or ATM cards as soon as you're aware they're missing.

Be Mindful of What You Share. It's not a good idea to post personally identifying information on social networking sites, or to give it out over the phone, unless you are certain with whom you are speaking. Before you provide personally identifying information, ask how it will be used and secured. Be sure never to print your driver's license, Social Security numbers, account numbers, or other sensitive information on your checks or on the outside of payment or deposit envelopes.

Use Caution Online. You can better protect your online accounts and transactions by using strong passwords that you regularly update. Use multi-factor authentication if available. Multi-factor authentication requires more than one method of identification to verify a user's identity. When you are finished with a secure session, remember to log off completely. If you shop online, transmit payment information via encrypted, secure websites that have an icon of a padlock in the address bar and a URL that starts with https. To understand a site's information handling practices, review privacy policies before using a site, and consider refraining from using a site if you are not comfortable with its practices.

Think twice before downloading files or clicking on emailed links or attachments that are unexpected or unfamiliar. Since email is generally unsecure, refrain from transmitting your Social Security number or other sensitive information by email, or transmitting it over the Internet (unless you are using an encrypted, secure website that you went to directly).

Be on the lookout for "phishing" sites, fraudulent sites that mimic real ones in order to capture users' personal information. Be wary of using public wireless "hotspots" that are not secure.

Protect Yourself When Using an ATM. Try to use a card with a "chip" feature; chip technology is more secure. When using an ATM, block it with your body to prevent "shoulder surfers" from stealing your personal information.

Be wary of using ATMs that look unusual or odd. Generally, private ATMs have less security protections than bank ATMs.

Remember to take your receipt. It may contain personal information, including your account balance. Before leaving the ATM, make sure you close out your transaction and have your card in hand. And of course, never share your PIN.

Protect Your Computer and Mobile Devices. To give yourself the most protection, it is advisable to install a firewall on your home computer to prevent hackers from obtaining personal identification and financial data from your hard drive; install and regularly update virus protection software to prevent malware from causing your computer to send out files or other stored information; and regularly install your browser's security patches.

If you have a wireless network, ensure that a password is required to access it. Ensure also that your computer, cell phone, blackberry, and other personal assistant devices are protected with a strong password.

Monitor Disclosures and Mail. Be aware of billing cycles, and review your statements regularly. If you don't receive bills on time, call the company. (Sometimes identity thieves change your billing address or divert your mail.)

In general, it's a good idea to limit receipt of sensitive postal mail where possible to avoid the chance it will be stolen. If you are planning to be away from home for an extended period of time, call the U.S. Postal Service and request "Hold Mail" service. Further, consumers can remove their names form marketing lists and opt out from receiving unsolicited offers of credit by calling 888-567-8688. Opting out will reduce the amount of solicitation mailings you receive.

Limit What You Carry. Take steps to minimize your exposure to identity theft in the event your wallet is lost or stolen by carrying only credit and debit cards that you absolutely need. Also, some medical and pharmacy benefit cards may contain Social Security numbers. If you have these, only carry them when you need to use them.

It's a good idea to memorize personal identification numbers (like your ATM PIN) and online passwords instead of keeping them in your wallet or purse.

Guard Your Social Security Number! Your Social Security number is an important piece of personal information, used by many entities as an identifier for tax filing, employment, credit reporting, and other purposes. Take steps to make sure it does not fall into the wrong hands.

When someone requests your number, ask why they need the number, and whether you can use an alternate identifier. It is not advisable to provide your Social Security number on checks, over the telephone in public, as a general form of identification, when making a purchase in a store, or by email.

Generally, employers, financial institutions (banks, credit unions, insurers) and the Internal Revenue Service (and other tax collection entities) may validly request your Social Security number.

Protect Your Medical Information. An identity thief can use a victim's name or health insurance information to obtain medical care and prescriptions, or file claims with an insurer. Medical identity theft can result in damaged credit, and impact a victim's medical treatment if the thief's medical treatment is included in a victim's medical records. Always remember to check all your health-related mail, email, and records, and to review statements and communications from your insurance company and health care providers for unfamiliar items and services, and for health conditions you don't have. Notify your insurer and provider if you see something wrong.

Protect Your Child's Information. A child's credit is extremely valuable to an identity thief. Safeguard your child's personal information, and educate him/her about online safety.