

information may have been stolen, are not careful with their personal information or have many family members using the same credit cards. Consumers should understand exactly what would be provided by an ID Theft Protection Service, before subscribing, as some of these services are available at no charge.

ID Theft Insurance: Identity theft insurance reimburses you for many of the costs associated with reclaiming your identity and restoring your good name, such as legal fees, lost wages from time taken off work to restore your identity, and postage expenses. This insurance does not fix your credit standing resulting from ID theft, but it may help you recover from this crime. It can be obtained through homeowners or renters insurance, as a stand-alone policy, or through your credit card company.

The coverage provided by this insurance varies greatly among insurers, therefore, you should understand exactly what you may be purchasing. In determining whether to purchase this insurance, you should note that an ID theft victim may pay thousands of dollars in out-of-pocket expenses to restore their identity, and could spend days clearing their record. You should consider whether you could benefit from insurance coverage for lost wages, since your employer may not authorize unpaid leave to handle ID theft. However, you should also recognize that a small percentage of ID theft victims require legal assistance to undo judgments and criminal records racked up by thieves in your name. Some credit card issuers make ID theft assistance available to cardholders for free.

Consumers who purchase ID theft insurance should continue to safeguard their personal financial information, since identity theft can still occur and tarnish your credit.

The best insurance is prevention.

July 2011

Call the New York Department of State's Division of Consumer Protection for consumer-related assistance or to file a complaint



Advocating for and Empowering
New York Consumers

New York State Department of State
Division of Consumer Protection

Consumer Assistance Hotline

1-800-697-1220

www.dos.ny.gov

A product of the New York Department of State Division of Consumer Protection's
Identity Theft Prevention and Mitigation Program

A Consumer Guide to

IDENTITY THEFT



**NEW YORK DEPARTMENT OF STATE
DIVISION OF CONSUMER PROTECTION**

ANDREW M. CUOMO
GOVERNOR

CESAR A. PERALES
SECRETARY OF STATE

INTRODUCTION

Identity theft is the most common consumer fraud complaint, and the fastest growing financial crime, affecting approximately 10 million Americans each year. It is of particular concern in New York, which has one of the highest per-capita rates of identity theft in the country. Some victims of identity theft have lost job opportunities, been refused loans, or been arrested for crimes they didn't commit. It could take victims of identity theft many hours and thousands of dollars to clear their name.

Identity theft occurs when your personal information such as date of birth, address, Social Security number, telephone numbers, credit card and bank account numbers and passwords are used by thieves. The criminals can then open new accounts in your name, apply for loans, make large purchases, drain your bank accounts and acquire your assets.

Identity theft costs consumers and businesses more than \$50 billion each year.

Anyone can be a victim of identity theft, including young children. Often times, parents of youngsters do not check with credit bureaus to request a credit report, or a "no activity" report, nor do they take steps to ensure that their child's personal information is kept secure. As a result, many young people are shocked to discover that their identity has been stolen and their credit ruined, before even having a chance to use their first credit card. Frequently, identity theft is committed by a person you know.

HOW ID THEFT OCCURS

Some of the most common ways your personal information is obtained include: recovering mail thrown in your trash; stealing business records or hacking into computers; and scamming information from you by posing as your bank, a legitimate business or a government official.

Warning Signs

Unfortunately, in many cases, it is hard to prove that theft of your identity has occurred. However, you should be concerned if:

- You receive bills for purchases you never made or collection notices regarding debts you did not incur.
- You are denied credit for no apparent reason.

4. Call the ID Theft Clearinghouse at 1-877-438-4338 to report the theft. The Federal Trade Commission manages and maintains the Clearinghouse. Counselors will provide additional consumer advice. The Clearinghouse provides law enforcement officers with a central database of identity theft complaints.

5. If personal checks are stolen or lost, notify the bank immediately and have a "stop payment" put on all of the missing checks. Ask your bank to notify the check verification service with which it does business. There are several companies providing check verification services. A listing of the major companies includes (this is a non-exhaustive list):

Certegy Check Services:	1-800-437-5120
ChexSystems:	1-800-428-9623
CrossCheck:	1-800-552-1900
	(have store number when calling)
Shared Check Authorization Network (SCAN):	1-800-262-7771
TeleCheck:	1-800-710-9898

6. If your driver's license or other government-issued identification has been stolen, contact the agency that issued the document. Follow its procedures to cancel the document and get a replacement. Contact the U.S. Postal Service if you suspect the identity thief used the mail.

7. If you are a senior citizen or a disabled person, you may be eligible for crime victim compensation from the NYS Office of Victim Services (OVS) to cover out-of-pocket expenses for financial counseling. Contact OVS at 1-800-247-8035.

ID PROTECTION SERVICES AND ID THEFT INSURANCE

Products and services are available to help protect your identity and compensate you for some costs in restoring your identity if you have been victimized.

ID Theft Protection Services: These services help you rapidly identify any changes to your credit report, thereby making it easier to detect identity theft. They generally offer credit report monitoring every business day, provide quarterly reports on changes in your credit report, and supply you with copies of your credit report. Many consumers may find these to be valuable services, particularly those who suspect that their personal

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

1. Contact the fraud departments of the three major credit bureaus:

Equifax:	1-800-525-6285
Experian:	1-888-397-3742
TransUnion:	1-800-680-7289

Inform these organizations that your identity has been stolen and ask that a “fraud alert” be placed on your file. This alert can help stop someone from opening new credit accounts in your name. Also ask for free copies of your credit reports and review them carefully to identify unauthorized accounts or charges.

There are two types of fraud alerts:

- An **Initial Alert** stays on your credit report for at least 90 days. This is appropriate if you suspect that you have been, or are about to be, a victim of identity theft. When you place an initial fraud alert on your credit report, you are entitled to one free credit report.
- An **Extended Alert** stays on your report for 7 years. This is appropriate if you’ve been a victim of identity theft and you provide the credit reporting company with an “identity theft report.” When you place an extended alert on your credit report, you are entitled to two free credit reports within 12 months from each of the three major credit reporting companies. When a business sees the alert on your credit report, they must verify your identity before issuing credit.

2. For any accounts that have been fraudulently accessed or opened, contact the security department of the creditor or financial institution and follow up in writing. Immediately close accounts that have been tampered with and open new accounts which require passwords in order to gain access to them.
3. File a report with the police department. Identity theft and fraud are felonies punishable by law. Keep a copy of the free police report to provide to credit card companies, banks and credit reporting agencies as proof that a crime was committed. Submitting a police report can block reporting of fraudulent data on your credit report. You can also gain access to transaction records of creditors by submitting a copy of a police report.

- You stop receiving monthly bank or credit card statements.
- Your credit report contains inaccurate or unfamiliar information.

HOW TO PROTECT YOURSELF

You can reduce your risk of becoming a victim of identity theft by carefully managing your personal information.

Safeguard Personal Information

- Keep personal information in a safe place. Store this information out of sight, especially if you employ outside help for work in your home or have roommates.
- Minimize use of your Social Security number. Provide your Social Security number only when absolutely necessary. Ask to use another type of identifying number whenever possible. When mailing a payment to a creditor, do not put your Social Security number or telephone number on your check. It is illegal in New York State for a business to require you to put account numbers or your Social Security number on a check. New York also prohibits your Social Security number from being used as a personal identifier, password or code on a membership or services card. An entity cannot require you to transmit your Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted. It is also illegal for anyone to intentionally disclose your Social Security number.
- Review your medical explanation of benefits statement regularly. Medical account information could be stolen and used by others.
- Limit information in your wallet. Carry only the credit cards you plan to use and only carry your Social Security card when absolutely necessary. Make copies and/or a list of everything in your wallet containing personal information.
- Determine how personal information will be used. Before revealing personal information, find out how it will be used and with whom it will be shared. Let companies know that you do not wish to have your personal information shared with anyone else.
- Place passwords on your credit card, bank and phone accounts. Avoid using common passwords or personal identification numbers (PIN) such as your mother’s maiden name, your date of birth, or your phone number.

- Properly dispose of documents. Dispose of any documents that contain your personal information by shredding or burning them. Make sure that pre-approved credit card offers and convenience checks are destroyed.
- Minimize use of mail for banking. Use direct deposit and pick up your personal checks from the bank whenever possible. This will reduce the likelihood that your account information and personal checks fall into the wrong hands.
- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your post office, instead of an unsecured mailbox. Remove mail from your mailbox promptly or use a locked mailbox or slot.
- Don't let your credit card out of your sight. Thieves may use handheld magnetic card readers to obtain personal information off the magnetic strip on credit and debit cards. Culprits have included waiters, gas station attendants, and store clerks.
- Be careful when using ATMs. When at an ATM, use caution and be wary of the people around you. Cell phones may be used to take a picture of your ATM or credit card. If an ATM is in a locked entry location, try to be the only one inside of the doors. Also, try to use only ATMs associated with banks. Some private or independent ATMs have been rigged to allow thieves to steal account numbers and PINs.
- Reduce unsolicited credit card applications. The fewer credit card applications you receive, the less likely a credit card will be stolen. Call 1-888-5OPTOUT to have your name removed from these marketing lists and opt-out of information sharing to non-affiliated companies by your financial institutions.

Use Computers Wisely

- Prevent unauthorized access to your computer. Some viruses can cause your computer to send your information to unknown parties. To help prevent such viruses, update your virus protection software regularly and don't download files from strangers or click on links from people you don't know. Use a firewall, especially if you have a high-speed or "always on" connection to the Internet.
- Take care in transmitting personal information. Use a secure browser. When submitting personal information, look for the "lock" icon on the status bar.

- Beware of "phishing." Phishing is the practice of sending bulk e-mail or pop-up messages that deceive consumers

More than 1,000 "phishing" web sites are created each month. Most are disconnected after only 3 days, making it difficult for law enforcement to track down the culprit.

- into disclosing their account numbers, passwords, Social Security numbers and other personal information. This often occurs through e-mail requests to "update" or "validate" records or accounts. The message may direct you to a web site that looks just like a legitimate organization's web site, but it isn't. To help address this, do not give personal information to someone who has called or e-mailed you unsolicited. Legitimate companies do not solicit information in this manner. Instead, confirm the legitimacy of the request by phoning or e-mailing the company first, using contact information on your account statement or in the telephone book.
- Try not to store sensitive information on your laptop. Laptops are easily stolen. Avoid using a feature that saves your user name and password on your laptop, and always log off when finished.
- Dispose of computers properly. Delete any personal information stored on your computer before disposing of it, by using a "wipe" utility program, which overwrites the hard drive.

Carefully Review Bills and Credit Reports

- Maintain accurate records of all banking and credit card accounts. A missing statement may mean that someone has obtained and re-routed your bills and financial information.
- Review your bills. Thoroughly review all bills before remitting payment. Unauthorized charges may be the first sign of identity theft.

- Review your credit reports. If an identity thief is opening new accounts in your name, these accounts are likely to show up on your credit report. New Yorkers may obtain a free credit report from each of the three national credit reporting agencies, once every 12 months. Visit www.annualcreditreport.com or

Many financial advisors suggest that consumers obtain one free credit report from a reporting agency at a time, spaced equally throughout the year. This may help you detect changes or new information and enable you to identify problems sooner than if all three credit reports are obtained at the same time.

call 1-877-322-8228 to request this free report. Carefully check your credit report for accuracy and ask the credit reporting agency to document and review any incomplete or incorrect information.