

Identity theft is the fastest growing crime in America today. Identity theft requires only a few pieces of valid personal information. With them, thieves can apply for and receive credit cards or debit cards in your name. Your credit can be quickly damaged and your efforts to correct these problems can become a nightmare.

The acquisition of key pieces of identity, such as name, address, date of birth, social security number and mother's maiden name, enable the impersonation to occur. This information allows the identity thief to commit numerous forms of fraud which include, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for credit cards, loans and social security benefits, renting apartments, and establishing accounts with utility and telephone service providers.

The identity thief has many ways to gain access to your information. It can be obtained from uncollected mail sitting in your mailbox, personal information carelessly thrown in the garbage, dishonest retail or restaurant employees or by the theft of your wallet or pocketbook.

How do the thieves assume your identity? They may rent a mailbox, usually at a package shipping center. Then, they fill out a change of address card on your account using the address from the center and the mailbox number. They begin running up charges on your accounts. The bills then go to the new address and you may not find out about it for a few billing cycles, if at all.

The thieves aren't going to pay the bills or they may just pay the minimum to keep the credit card company "happy", prolonging the time it takes for you to find out about the problem. When they stop paying the bill all together or write bad checks, the delinquent accounts appear on your credit report.

How to prevent becoming a victim:

- ◆ Shred all bills, credit card charge receipts, credit applications, insurance forms, bank statements, expired charge cards, and pre-approved credit offers before throwing them into the garbage.
- ◆ Do not provide personal information simply because someone asks for it or because it is asked for on a form, questionnaire or product registration card.
- ◆ Do not give out your social security number freely.
- ◆ Promptly remove mail from your mailbox. If going on vacation, make arrangements for someone to take the mail for you or call the U.S. Postal Service at 1-800-275-8777 and request a "vacation hold" for your mail.
- ◆ Place outgoing mail in post office collection boxes or at your local post office.
- ◆ Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number or bank PIN number, unless you initiated the call. Make sure you release this information only when necessary.
- ◆ Don't carry extra credit cards in your wallet or pocketbook. Cancel the ones you no longer use.
- ◆ Order credit bureau credit reports once a year to check for fraudulent activity or other discrepancies.
- ◆ Sign all new credit cards upon receiving them in the mail.
- ◆ Save all credit card receipts and match them against your monthly bill.
- ◆ Never leave receipts at an ATM, store counter, self-serve gas pump or in trash cans. Keep track of all paperwork and destroy those you no longer need.
- ◆ Memorize your social security number and passwords. *Never* write them down or carry them in your wallet or pocketbook.
- ◆ Keep track of when routine financial statements should arrive in the mail. Contact the issuing bank or company, if one doesn't arrive. Review statements to verify all charges.
- ◆ Never loan anyone your credit cards.
- ◆ If a credit card you applied for doesn't arrive in a timely fashion, notify the issuing bank. Also keep track of expiration dates on your cards. If the new card doesn't arrive notify the issuing bank.
- ◆ Notify all banks and credit card companies of any change of address.
- ◆ Never put bank account or credit card numbers on the outside of an envelope or postcard.
- ◆ Beware of telephone solicitations asking for personal information about your accounts or your social security number.
- ◆ When disclosing credit card, checking account or other financial data online, use caution. Make sure you receive a secured authentication key (lock icon) and a statement that indicates your transaction is secure.
- ◆ Be cautious of e-mails and instant messages that are unsolicited and request you to confirm credit card numbers, passwords or other personal information. Con artists often pose as agents of banks, on-line shopping services or internet providers attempting to obtain this information to commit fraud.
- ◆ Financial institutions may share your information with other companies. If you want, you can limit some of that sharing. Each year, your financial institutions should send you a privacy notice with instructions for "opting out." Read these notices carefully. Also, when establishing accounts with new companies, ask about privacy policies and make your wishes known.
- ◆ The credit bureaus offer a toll-free number that enables you to "opt-out" of having pre-approved credit offers sent to you for two years. Call 1-888-5-OPTOUT, (567-8688) for more information.

- ◆ The Federal Government has created the National Do Not Call Registry. To register, or get information, visit www.donotcall.gov, or call 1-888-382-1222 from the phone you want to register. You will receive fewer telemarketing calls within three months of registering your number. It will stay in the registry for five years or until it is disconnected or you take it off the registry. After five years, you will be able to renew your registration.

What to do if you become a victim:

- ◆ Contact all creditors, by telephone and in writing, to inform them of the situation.
- ◆ Notify the Police.
- ◆ Alert all banks to flag your accounts and to contact you for unusual activity. Change all passwords and PIN numbers.
- ◆ Document all contacts and keep copies of all correspondences.
- ◆ Contact the Social Security Administration Fraud Hotline at 1-800-269-0271.
- ◆ Contact the Department of Motor Vehicles to have a new license number issued in your name.
- ◆ Call the nearest U.S. Postal Inspection Office.
- ◆ Call the Federal Trade Commission's identity theft hotline at 1-877-438-4338 and file a complaint.
- ◆ If you are the victim of identity theft, call each credit bureau with a national database and ask to have a "Fraud Alert/Victim Impact" statement placed in your credit files. Also request that all creditors contact you before they open any new accounts in your name. The following contact information is provided to assist identity theft victims:
 1. Equifax www.equifax.com 1-800-685-1111
 2. Experian www.experian.com 1-888-397-3742
 3. Trans-Union www.tuc.com 1-800-916-8800
- ◆ If you are a victim of check fraud, you should contact the following:
 1. Telecheck 1-800-710-9898
 2. Equifax 1-800-437-5120



NEW YORK CITY POLICE DEPARTMENT

WHAT YOU NEED TO KNOW ABOUT...

Prepared by:

Office of the Chief of Department

Crime Prevention Section

34 ½ East 12th Street

New York, NY 10003

(212) 614-6741

&

Detective Bureau

Special Frauds Squad



You can help us fight terrorism,
report suspicious activity to:

1-888-NYC-SAFE

1-888-692-7233

IDENTITY THEFT

Dial 911 for Police Emergencies

Dial 311 for Non-Emergency City Services