What to Do If You Are a Victim of Identity Theft

If you have been victimized by identity theft, you should take certain steps to protect yourself and minimize the consequences. Correcting the damage to your credit rating and good name may be a tedious and time consuming process. As you speak to the contacts listed below, write down the names of the people you talk with, their positions, their responses, and the dates and times of your conversations. When sending correspondence through the mail, keep copies, and use registered mail with a return receipt requested. The post office can help you with the procedures for registered mail.

The Chicago Police Department can take a report over the phone if you call 311, or you may go to the nearest District Station.

Once the report is made, it will take approximately two to five days for a detective from the appropriate Property Crimes Unit to be assigned to the case. Shortly thereafter the assigned Detective will contact you to start the follow-up investigation.

The Financial Crimes Investigations Unit of the Chicago Police Department investigates identity thefts of a complex and involved nature, and identity theft investigations are normally referred to this unit by one of the Property Crimes Units.

Next, contact the three credit reporting agencies:

Experian

www.experian.com

1-888-Experian (397-3742)

www.equifax.com

Equifax Fraud Victim 1-800-525-6285

TransUnion Fraud www.tuc.com

1-800-680-7289

When speaking to these agencies, you should:

Notify all three credit bureaus and advise them of the identity theft.

Request a copy of your credit report from each bureau. Request that a "hawk" alert/fraud alert be placed on your credit report.

Request that all inquiries on your credit report be reported to you.

After viewing your credit report, contact all banks, credit card companies, etc. where fraudulent credit has been established.

File affidavits of forgery with all banks/creditors where credit has been established. Contact the bank or creditor for procedures on how this is done.

Request copies of your credit report every six months until your credit is clear.

Request that a consumer statement be placed on your report (it may have to be in writing). A consumer statement is an explanation of your credit problems.

Contact all the utility companies that provide service to you to ensure that no other accounts are applied for or established in your name. The companies would include, gas, electricity, cable, water (City of Chicago), phone (cellular companies, as well as standard phone), etc.

Contact the companies first by telephone and send a letter to each company by registered mail with a return receipt, giving your name and your authorized accounts. Be sure to state that no other accounts in your name are authorized. The easiest way to do this is to create a form letter, with your name and address where the addressee and account number can be inserted as appropriate. Also, use personal ID numbers whenever possible to activate your accounts.

The Privacy Rights Clearinghouse at 619-298-3396 offers tips for resolving problems associated with financial fraud.

The following agencies are some of the law enforcement agencies that also investigate identity theft cases.

Illinois State Police www.isp.state.il.us

Department of Justice www.usdoj.gov

Federal Bureau of Investigation www.fbi.gov

Identity Theft Hotline 312-781-4545

Internal Revenue Service www.treas.gov/irs/ci

(800) 829-1040

U.S. Customs Service www.cbp.gov (312) 983-9500

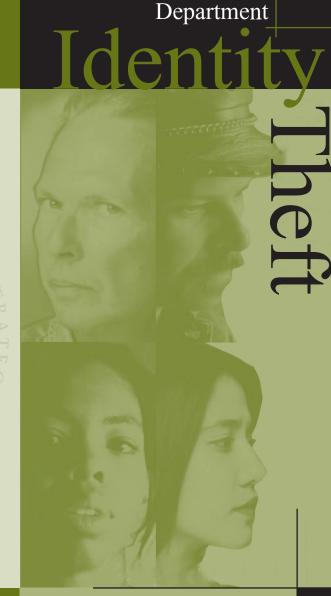
U.S. Postal Inspection Service www.usps.com/postalinspectors (312) 983-7900

> U.S. Secret Service www.treas.gov/usss/ (312) 353-2774

Social Security Administration www.socialsecurity.gov (312) 353-7815

For a complete list of agencies and other resources please visit our web page.

www.chicagopolice.org



Chicago Police



City of Chicago Rahm Emanuel Mayor

Department of Police Garry F. McCarthy Superintendent



Identity theft is the unauthorized use of personal identifying (ID) information, such as a name, date of birth, or Social Security number, to commit financial fraud. It can encompass a number of crimes, from the unauthorized use of credit cards to a complete takeover of another person's name and financial accounts. An identity thief may use someone's personal identifiers to illegally obtain credit cards, open checking accounts, apply for loans, rent or purchase residences, establish services with utility companies, or engage in other fraudulent activity.

By Illinois State Statutes, financial identity theft occurs when a person knowingly uses someone's personal IDs or documents to fraudulently obtain credit, money, goods, services, or other property in the name of that person.

"Personal IDs" may include name, address, telephone number, birth certificates, Social Security cards, credit cards used as IDs, etc.

"Credit" may include credit cards used to make purchases, debit cards, automobile loans, etc.

"Money" may include cash, loans, insurance benefits, unemployment benefits, second mortgages, etc.

"Goods" may include tangible items, such as computers, automobiles, etc. "Services" may include bank accounts, utility services, etc.

"Other property" may include real estate, apartment rentals, or anything that does not fall into the other four categories.

Preventing Identity Theft: Do's and Don'ts

Who are the Victims of Identity Theft?

Identity theft can claim many victims. Credit grantors, such as banks and retail merchants, are victims when they finance the selling of goods and services that are not paid for. A person whose identity has been stolen is a victim, even if protected by insurance coverage or credit card reimbursement provisions. Although they may not have out-of-pocket losses, identity theft victims may suffer from injuries to their reputations, and may have to go through lengthy and often agonizing processes to reestablish credit.

How Identity Theft May Occur

People who commit financial identity theft do not fit a stereotype. The offender may or may not be known to the victim, and the method of operation varies. Information may be obtained by searching through trash cans at banks, mortgage firms, social or credit agencies, public record agencies, obituaries, or residential garbage cans. Financial-related mail, such as credit statements, bank statements, or pre-approved credit card applications can be stolen from mailboxes. Identity thieves who work at car dealerships, mortgage houses, collection agencies, or utility services may have easy access to credit reports, and those employed as telephone marketers or mail clerks may have access to other financial information or documents. Information can sometimes be found on the Internet or through commercial databases that are accessed for a fee.

DO:

Protect your incoming and outgoing mail. Remove your mail from the box as soon as possible. If you believe that mail containing personal or financial information was opened or altered, notify the sender and stay alert for any suspicious activities, such as phone calls to verify your credit card numbers, loans, or bank accounts. If you are expecting a new or renewed credit card or other financial document by a certain date, watch the mail to be certain it arrives, and pursue the matter if it fails to arrive.

Shred or completely tear up any discarded paperwork that contains personal identifiers or financial information, including pre-approved credit card applications. If a vendor uses carbon copies for credit card bills, ask for and destroy the carbons. You can lessen your risk even further by discarding destroyed documents in separate garbage cans.

Be aware of where your personal identification is kept and who has access to it. Protect your wallet and purse and never leave them unattended.

Closely review your bills, including utility bills and bank statements, to ensure that all balances and receipts match and no activity is unaccounted for. If you do not get a statement or bill, find out why it is missing.

We also advise you to install software on your computer, available at most computer stores, that encrypts information you send in an e-mail. You can also ask your financial institution to add security to your accounts, such as special passwords.

Stop pre-approved credit offers by calling all three credit reporting bureaus and opting out of the programs. By opting out, you receive fewer pre-approved loans and credit applications.

DON'T:

Do not give out personal information in response to unsolicited offers by phone, mail, Internet, or in person. Criminals may pose as legitimate business people, charity workers, or law enforcement officers to gain your trust.

Do not use your Social Security number unless you have to, including on your driver's license and checks. The Illinois Secretary of State allows drivers the option of not having their Social Security number on the driver's license.

Do not fill out warranty cards for items you purchase or enter sweepstakes. Such information is often sold to others as a marketing tool.

Personal identifiers, account numbers, and other private information should not be provided to anyone, unless you know the information will be secure.

If you follow these steps, you will reduce your risk of being a victim of an identity theft, but you can not completely eliminate the risk. Your goal should be to reduce other people's access to your information, so you should know what people and companies do with the information you give them. Keep these facts in mind:

- Know the person or company to whom you give information
- Ask what the person or company will do with the information
- Err on the side of caution—keep an eye on your financial picture, so if irregularities occur you will recognize them.
- Remember: Although you may not have to pay