

What is identity theft?

Identity theft is a serious problem affecting millions of people each year. It involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

Is identity theft a crime?

New Jersey is one of forty three states which do in fact have a statute for identity theft. In the State of New Jersey, identity theft is covered under the wrongful impersonation statute.

(Wrongful Impersonation: 2C:21-17)

Wrongful impersonation escalates from a disorderly persons offense to a crime when the total monetary values for the goods or services that were defrauded exceeds \$200.00.

Most identity crimes will be multi-jurisdictional in nature. Frequently, you will not even realize that your identity was compromised until you receive a bill, statement, or some other notice that alerts you to the fact that you have a problem. Many times this is months after your identifiers were first stolen. The subsequent fraudulent use of your identifiers may very well have occurred in a different state.

How does identity theft occur?

Offenders who commit identity theft may or may not be known to the victim. There are many ways the offender may obtain your personal information or information related to your personal financial accounts. Information can be obtained from trash bins or at places where you conduct your personal business. It can be obtained from identity thieves who work at banks, mortgage firms, social or credit agencies, city-state-federal agencies, auto dealerships, collection agencies, utility service providers, telemarketers, doctor's offices, merchants and other businesses that have access to your personal information or credit card information. Identity thieves also contact victims via telephone and e-mail requesting personal information. Information can also be obtained from obituaries and taken out of residential garbage cans, mailboxes and mail facilities. The information obtained from these sources is used to assume a false identity.

Preventing Identity Theft

The Do's and Don'ts for preventing identity theft.

DO:

Order a copy of your credit report every year from all three of the major credit reporting agencies in order to check for fraudulent activity or discrepancies. In the State of New Jersey, you can obtain one free report each year from each of the credit reporting agencies.

Protect your mail by removing it from your mailbox as soon as possible. Consider using a locked mailbox.

Shred any discarded paperwork that contains personal identifiers or financial information, including pre-approved credit card and loan applications. If a vendor uses carbon copies for credit card bills, ask for and destroy the carbons.

Stop pre-approved credit offers by calling the Credit Reporting Industry at 1-888-567-8688.

Know where your personal information is kept, who has access to it, and who you may have provided it to in the past. Protect your wallet and purse and never leave them unattended. Keep an eye on your credit card when using it to pay for purchases.

Be aware of your surroundings when using ATM cards, making credit card purchases, using telephone credit card numbers and utilizing pin numbers or passwords.

Carefully review your bills, bank statements, credit card statements and other financial accounts, to ensure that all balances and receipts match and no activity is unaccounted for.

If you use a computer, install virus protection and firewall software to discourage hackers. Be aware of personal information that you send over the internet that could be viewed by others.

Destroy computers, hard drives, zip-drives, floppy disks, compact disks, or any other electronic device which may contain personal information before disposing of them.

Request your financial institutions to add security to your accounts, such as a special password.

DON'T:

Do not give out personal identifiers or financial identifiers in response to unsolicited offers by mail, phone, internet, and/or in person. Identity thieves frequently pose as legitimate business people, charity workers, or law enforcement to gain your trust.

Do not fill out personal information on warranty cards and sweepstakes entries; it is often sold to others as a marketing tool.

Do not provide or use your social security number unless you have to.

Do not provide personal identifiers, account numbers or other personal information unless you know the information will be secure.

Following these steps will reduce your risk of being a victim of an identity theft. Your goal should be to reduce other people's access to your information.

Remember: It is your responsibility to correct credit errors and restore your identity.

What do I do if I become a victim of identity theft?

Credit Bureaus:

- Immediately call the fraud units of the three credit reporting companies - Equifax, Experian and Trans Union. Report the theft of your credit cards or identity to them. Ask that your account be flagged and have a "Fraud Alert/Victim Impact" statement placed on your credit file, asking that creditors call you before granting credit. Obtain the names and phone numbers of businesses with whom fraudulent accounts have been opened.
- Review your credit report with them and request a copy.

Credit Bureaus		
Equifax	Experian	Trans Union
P.O. Box 105873	P.O. Box 949	P.O. Box 390
Atlanta, Ga. 30348-5873	Allen, Tx. 75013-0949	Springfield, Pa. 19064-0390
Credit 1-800-997-2493	Credit 1-888-397-3741	Credit 1-800-916-8800

Fraud 1-800-525-6285	Fraud 1-888-397-3742	Fraud 1-800-680-7289
www.equifax.com	www.experian.com	www.tuc.com

Creditors:

- Contact your creditors and those who provided credit fraudulently, by phone and in writing to inform them of the problem. Ask for replacement cards, close old or fraudulent accounts, obtain new account numbers and pin numbers if the accounts have been used fraudulently.

Federal Trade Commission (FTC):

- Contact the FTC and file a report either through the FTC web site (www.consumer.gov/idtheft) or by telephone 1-877-ID-THEFT. The FTC is the clearinghouse for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft.
- Obtain an "Identity Crimes Affidavit" and complete it. It will be useful when notifying merchants, financial institutions, credit bureaus, and it will assist the police.

Law Enforcement:

- Contact your local police department, file a report and obtain a case number. Most credit and financial institutions will require that you make a police report.

Assisting Law Enforcement with Your Case:

- Set up a folder to keep a detailed history of the crime. Keep a log of all contacts and make copies of all documents. Provide this information to the police and assist them with obtaining additional information.
- Gather all evidence and documentation of your financial loss and provide it to the police.
- Obtain suspect information or descriptions and provide it to the police.
- Obtain possible witness information, the salesperson, apartment managers, employers and persons who accepted the fraudulent applications or documents. Provide this information to the police.
- Complete FTC "Identity Crimes Affidavit" and provide it to the police.

Stolen Checks:

- If you have checks stolen or accounts set up fraudulently, report it to the bank and close the accounts. Set up new accounts and put stop payments on the outstanding fraudulent checks.
- Report the stolen checks to the check verification companies.

National Check Fraud Service	1-843-571-2143
SCAN	1-800-262-7771
TeleCheck	1-800-710-9898
CheckRite	1-800-766-2748
CrossCheck	1-707-586-0551
Equifax Check Systems	1-800-437-5120
International Check Services	1-800-526-5380

ATM Cards:

- If your ATM card is stolen or compromised, get a new card, account number and password.

Fraudulent Change of Address:

- Notify the local US Postal Inspector if you suspect someone fraudulently changed your address. Find out what your address was changed to. Notify the local Postmaster for that address and instruct them to forward all mail addressed to you to your correct address.
- The phone numbers for U.S. Postal Inspectors and Post Offices can be obtained in the phone book under Federal Government or through their web site, (www.usps.gov/postalinspectors).

Social Security Number:

- If your Social Security number has been used fraudulently, contact the Social Security Administration at 1-800-269-0271, or through their web site (www.ssa.gov/oig).

Drivers License Fraud:

- If you suspect that your drivers license or registration was lost, stolen or fraudulently used contact the New Jersey Division of Motor Vehicles. You will have to appear in person at a regional office and fill out a fraud affidavit. You must bring forms of identification and all proof to show fraudulent activity. You can locate your regional office by calling NJ DMV at 1-609-292-6500 or visiting their web site, (www.state.nj.us/mvc).

Passport Fraud:

- Protect yourself from passport fraud. Contact the U.S. State Department at their web site (www.travel.state.gov) and alert them that you were the victim of identity theft. Request that they alert you if anyone attempts to use your identity to acquire a passport.

False Civil and Criminal Judgments:

- Contact the Court where the judgment was entered and report that you are the victim of identity theft.

Personal Property Security:

- If you suspect that your identity was compromised by someone who had access to your residence, change the locks to your residence and vehicles if necessary.

Utility Companies:

- Contact your local utility companies to see if there is any unusual activity on your accounts.

Federal Laws that provide you protection from identity theft.

Identity Theft and Assumption Deterrence Act of 1998

Anyone who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or constitutes a felony under any applicable State or local law.

Fair Credit Reporting Act:

This act establishes procedures for correcting mistakes on your credit record and requires that your credit record only be provided for legitimate business needs.

Fair Credit Billing Act:

This act establishes procedures for resolving billing errors on your credit card accounts. It also limits a consumer's liability for fraudulent credit card charges. When proper notice is given the consumer's liability is limited to \$50.00.

Fair Debt Collection Practices Act:

This act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.

Electronic Fund Transfer Act:

This act provided consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.

For additional information:

<http://www.justice.gov/criminal/fraud/websites/idtheft.html>