



Readington Township Police Department

IDENTITY THEFT VICTIM'S REFERENCE GUIDE

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 a name, address, date of birth, or social security number, in order to impersonate them.

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.

What do thieves do with your information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Is identity theft a crime?

In the State of New Jersey, identity theft is covered under the wrongful impersonation statute. (**Wrongful Impersonation: 2C: 21-17**) 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 or country.

Clues that someone has stolen your information:

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- You receive statements for credit cards you did not apply for.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

Preventing Identity Theft:

The **DO'S** and **DON'TS** for preventing identity theft.

DO:

- Review your financial statements monthly and check carefully for fraudulent activity. Report any suspicious charges immediately.

Bonus Tip: Sign up for alerts and limit your credit card activity to a specific geographical area.

- Sensitive documents should be kept in a safe. Credit and debit cards should be securely placed in your wallet at all times. For added security, use a RFID blocking wallet or card sleeve.

Bonus Tip: Shred all aged documents that contain sensitive information

- Use two-factor identification for all online accounts.

Bonus Tip: Never elect to have your device “Remember your password for a that involves payment of any kind.

- Invest in a strong anti-spyware program to protect your hardware from hackers.

Bonus Tip: Encrypt your hard drive for an extra level of protection.

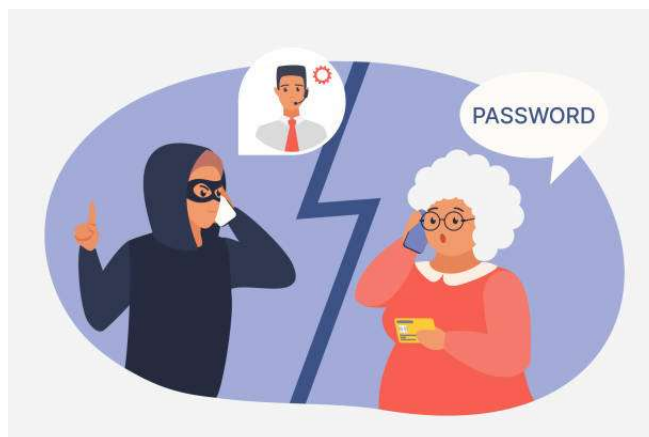
- Use different, strong passwords for each of your accounts and devices.

- Protect your mail by removing it from your mailbox as soon as possible.

Bonus Tip: Consider using a locked mailbox.

- Stop pre-approved credit offers by calling the Credit Reporting Industry at **1-888-567-8688** or **www.optoutprescreen.com**

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



DON'T:

- Don't 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.
- Don't give away more information than necessary: Your bank and credit card provider already know your PIN number and address. They don't need you to tell them via email, phone, or web page.
- Don't open suspicious looking emails or click links for unfamiliar sites.
- Avoid public Wi-Fi: Public Wi-Fi is a great hunting ground for thieves. Avoid if possible. At the very least, avoid all online banking or password logins while using public Wi-Fi.

Bonus Tip: Secure your own home Wi-Fi with a strong password.

- Don't share passwords, email accounts or any other online personal data with other people: it is much harder to protect when more than one person has access.
- Don't carry extra credit cards in your wallet or purse: cancel the ones you no longer use.



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” 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 Bureau contact information:

Equifax P.O. Box 105873 Atlanta, GA 30348-5873 Credit Report, 1-800-997-2493 Fraud Alert, 1-800-525-6285	 www.equifax.com
Experian P.O. Box 949 Allen, TX 75013-0949 Credit Report, 1-888-397-3741 Fraud Alert, 1-888-397-3742	 www.experian.com
Trans Union Union P.O. Box 390 Springfield, PA 19064-0390 Credit Report, 1-800-916-8800 Fraud Alert, 1-800-680-7289	 www.tuc.com

Creditors: Contact your creditors and those who provided credit fraudulently, 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.

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.

Federal Trade Commission (FTC):

- Contact the FTC and file a report either through the FTC website (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.



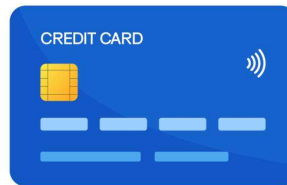
Stolen checks:

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



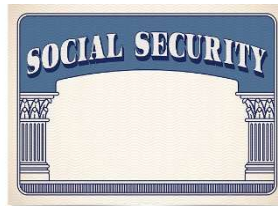
Debit/Credit cards:

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



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 website: oig.ssa.gov/report/.



Driver's 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 can locate your regional office by visiting the NJMVC website, (www.nj.gov/mvc).



Passport fraud:

- Protect yourself from passport fraud. Contact the U.S. State Department at their website (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 judgements:

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



Utility companies:

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

