Identity Theft

Handbook

www.NJConsumerAffairs.gov ■ 1-800-242-5846

Identity Theft occurs when someone uses your personal information without your permission to commit fraud. Identity theft can wreak havoc on your finances, credit history, and reputation and may require time, money, and patience to resolve. Your identity can be stolen in different ways. Please review the information in this booklet to familiarize yourself with the types of identity theft and learn how to protect yourself and loved ones from becoming victims.

Be an Informed Consumer…*We can Help!*

A CONSUMER GUIDE TO IDENTITY THEFT

table of contents

Signs that you may be a victim of Identity Theft

- Your bank account lists unauthorized transactions or withdrawals.
- You unexpectedly get denied for a credit card, a loan or other service.
- Your electronic payments and/or checks are rejected.
- You receive calls from debt collectors about debts that are not yours.
- You are unexpectedly no longer receiving your regular mail.

- You find unfamiliar accounts on your credit report.
- You receive mail, including bills, statements and/or legal correspondence, for goods or services that you did not purchase.
- Your health plan unexpectedly rejects your medical claim because the records show you have reached your benefits limit.

Identity Theft comes in many different forms. Familiarize yourself with the various types of identity theft so that you know how to protect yourself from becoming a victim.

Financial Identity Theft

Social Security Identity Theft

Medical Identity Theft

Tax Identity Theft

Elder Identity Theft

Child Identity Theft

Driver's License Identity Theft

Financial Identity Theft

Financial Identity Theft occurs when someone uses another person's financial information to commit fraud. For example, someone may try to trick you into disclosing your credit card number or bank account number so that they can use this information to open credit card accounts, make purchases or commit other frauds. This is the most common form of identity theft.

Early detection is crucial when it comes to fighting financial identity theft. The sooner you realize your identity has been stolen, the sooner you can correct problems and prevent further damage. The best way to protect against financial identity theft is to regularly check your financial accounts and statements, and immediately contact your financial institution if an unauthorized charge appears.



Social Security Identity Theft

Social Security Identity Theft occurs when someone uses your Social Security Number to commit fraud or other crimes. Your Social Security Number can be used for a variety of fraudulent purposes, including:

- Opening new financial accounts
- Filing a fraudulent tax refund
- Stealing your unemployment or social security benefits
- Obtaining medical care

Always guard your Social Security Number so that it does not get into the wrong hands.

To report a lost or stolen Social Security Number, or if you believe your Social Security Number has been used fraudulently, contact the Social Security Administration at **1-800-269-0271** or visit the Office of the Inspector General's webpage: **https://oig.ssa.gov/report-fraud-waste-or-abuse/**.

Medical Identity Theft

Medical Identity Theft occurs when someone uses your personal information, such as your Medicare Identification Number, in order to obtain medical care, buy medication, access your medical records, or submit fake claims to your insurer or Medicare in your name.

Medical Identity Theft can have devastating consequences

Loss of health coverage: Fraudulent medical claims can max out your medical benefits, causing you to be denied benefits.

Negative credit history: Fraudsters can build up large bills at hospitals in your name and then disappear without a trace. Eventually, the fraudulent bills go to collection. You might not even realize your identity was stolen until bill collectors start contacting you.

Inaccurate medical records: When an identity thief uses your health insurance to get medical care in your name, doctors may update your records with the imposter's medical information, resulting in incorrect entries in your medical history. Erroneous entries can be extremely dangerous, as medical personnel rely on this information to prescribe medicine and give treatments.

Higher premiums: Your premiums may rise as a result of these fraudulent medical claims.

Difficulty obtaining life insurance: You may have a hard time qualifying for life insurance if the premiums are based on the imposter's health records rather than your own.

How to recognize Medical Identity Theft

Review your Explanation of Benefits statements or Medicare Summary Notices: Review these documents regularly to make sure the claims match the services you received. Report questionable charges to your health insurance provider or Medicare. If you are sent bills for medical services you did not receive, call the provider and dispute the charges.

Check your medical records: If you think you may be a victim of Medical Identity Theft, carefully review a copy of your medical records for any inaccuracies, including any incorrect medical diagnoses.

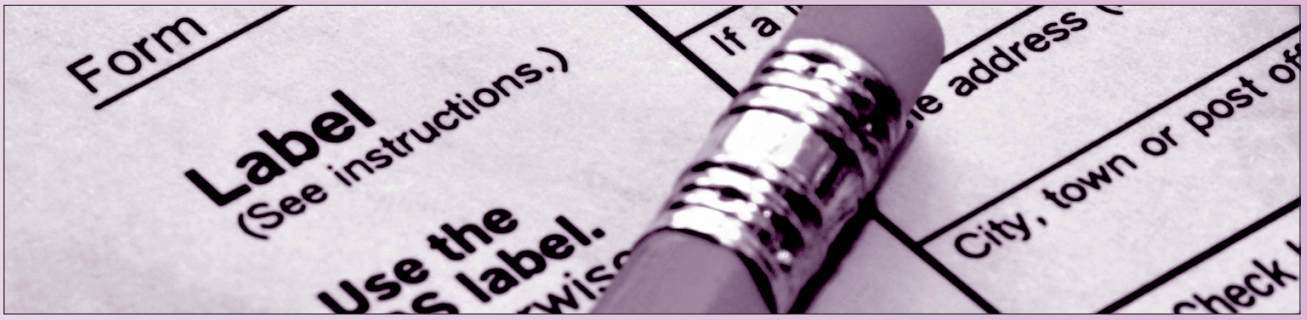
Report Medical Identity Theft

If you believe that you have been a victim of Medical Identity Theft, you should take the following steps:

- Immediately call your health insurance company's fraud department and your treating physician to report the theft.
- File a report with the NJ Office of the Insurance Fraud Prosecutor at **www.njinsurancefraud2.org/** or call **1-877-55-FRAUD**.
- File a report with the Medicaid Fraud Control Unit of the NJ Office of the Attorney General at **www.nj.gov/oag/medicaidfraud/** or call **1-609-292-1272**.
- Report Medicaid Fraud to the Medicaid Fraud Division of the Office of the State Comptroller by calling **1-888-937-2835** or visit **www.nj.gov/comptroller/divisions/medicaid/**.
- To report Medicare Fraud, visit: **www.medicare.gov/forms-help-resources/help-fight-medicare-fraud/how-report-medicare**
- Be sure to get copies of your medical records and work with your doctor's office and insurance company to correct erroneous information.

Tax Identity Theft

Tax Identity Theft occurs when someone uses your personal information (such as your Social Security Number or tax preparation software account username or password) to file a tax return in order to claim a fraudulent refund or establish a "verified identity" with tax authorities. You may not be aware of the problem until you attempt to file your tax returns and then learn that a return has already been filed. **The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.**


Form
Label
(See instructions.)
Use the
label.
City, town or post

How to Protect Yourself from Tax Identity Theft

- **NEVER** provide any personal information in response to an unsolicited phone call, email, social media message or text message claiming to be the IRS. The IRS will not make initial contact with consumers using these methods.

- **BEWARE** of emails, texts or social media messages that look like they're from the IRS or a financial institution. This is called *"phishing"* and the goal is to get you to provide personal information or click on links that either lead to fake websites or install malicious software on your computer.

- ***NEVER*** reply to, or click, on any links in suspicious email, texts, and social media messages.

- **ALWAYS** read correspondence from tax authorities.

- **ALWAYS** report suspicious activity to the IRS.
  Visit: **www.irs.gov/identity-theft-fraud-scams**.

- If possible, file your income taxes early in the season, before someone can file fraudulent taxes in your name.

- If you suspect you are a victim of Tax Identity Theft, continue to pay your taxes and file your return, even if you must do so by paper.

Report Tax Identity Theft

If you suspect you have become a victim of Tax Identity Theft, or if the IRS sends you a letter or notice indicating a problem, the Federal Trade Commission (FTC) suggests that you take the following steps:

- File a report with the FTC at **IdentityTheft.gov**.
- Contact one of the major credit reporting bureaus to place a "fraud alert" on your credit records. For even greater protection, consider a credit freeze. *See page 35 for further information regarding credit reporting bureaus.*
- Contact your financial institutions and close any accounts opened without your permission or that show unusual activity.

- If you receive an IRS notice in the mail that says someone used your Social Security Number to get a tax refund, follow the instructions provided in the notice. Visit **www.irs.gov/newsroom/taxpayer-guide-to-identity-theft**. If these steps don't resolve your situation, contact the IRS for specialized assistance at **1-800-908-4490**.

- If you suspect that you are a victim of tax fraud and would like to report the incident to the New Jersey Division of Taxation and have your account noted that you are a victim of identity theft or to identify any questionable activity, you should complete an Identity Theft Declaration form. For further information, visit: **www.state.nj.us/treasury/taxation/identity_theft.shtml**.

Elder Identity Theft

Elder Identity Theft occurs when someone wrongly obtains the personal information of an elderly person. Unfortunately, seniors can be especially vulnerable to identity theft scams as they may be isolated or unfamiliar with the latest scams. They are also often more reluctant to report identity theft because they might not know how to report it or are embarrassed about being victimized.

Steps to take to avoid becoming a victim of Identity Theft

- **NEVER** disclose any personal information over the phone. Seniors are often targeted by callers trying to trick them into giving out personal information, such as credit card and Social Security Numbers. These calls often take the form of the "grandparent scam," "romance scam," or "sweepstakes scam." Screen your calls. Only answer calls from people and businesses you know and trust. Let all unknown callers leave a message.

- **Secure all important documents,** such as bank statements and benefits statements.

- **Be safe online:** Emails and texts aimed at tricking the recipient to click on a link or open an attachment are often targeted at the elderly.

- **When using social media, do NOT share personal information** in your profiles, such as birthdates, vacation plans or health information.

- **Always guard your Social Security and Medicare Numbers.**

Child Identity Theft

Child Identity Theft occurs when a child's Social Security Number or other information is used to commit fraud or other crimes. Often, this information will be used to open credit accounts, apply for loans or government benefits. Child Identity Theft can go undetected for years, with victims unaware until they apply for a driver's license, first loan, or a job.

Steps you can take to protect your children from Identity Theft

- Check with the credit reporting bureaus to see if your child has a credit report. If so, review it carefully. Report any inaccuracies to the Federal Trade Commission and file a report with your local police department. You may also want to place a security freeze on your child's credit report. *See page 35 for further information regarding the credit reporting bureaus.*

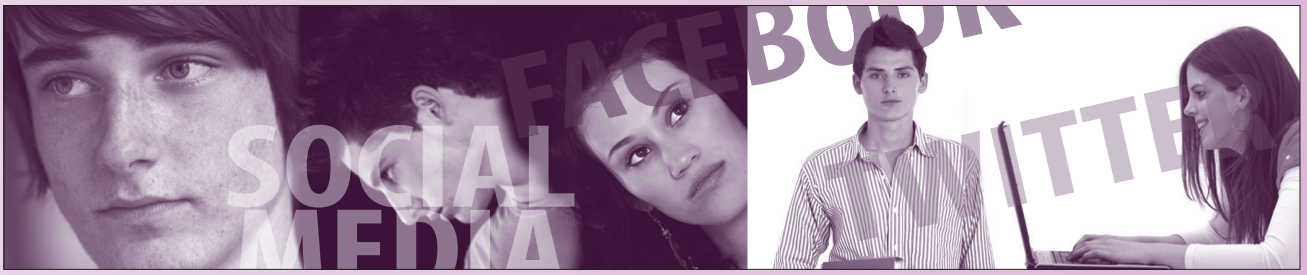
- Keep your child's personal information private, including name, address, birthdate, school and Social Security Number.

- Monitor how your child's school uses your child's personal information.

- Monitor your child's online activity and social media presence.

Warning signs that may indicate Child Identity Theft

- Your child receives pre-approved offers of credit or insurance in the mail in their own name.
- Your child receives promotional or junk mail.
- Your child is denied governmental benefits and/or financial aid because the benefits are already being paid to someone else using the same Social Security Number.


SOCIAL
MEDIA
FACEBOOK

Driver's License Identity Theft

Driver's License Identity Theft occurs when someone uses your identity, or submits false identity documents in order to obtain a fraudulent driver's license. Once someone has your license or obtains one fraudulently using your identity, it becomes easy to get other forms of ID in your name.

If someone using your identity gets pulled over for a traffic violation or drunk driving and gives the police officer your identity, their driving-related offenses might be added to your driving record, which can result in a revocation or suspension of your driver's license. These offenses can wreak havoc on your life and impact car insurance rates or any attempts to obtain new car insurance.

If you suspect your driver's license was lost, stolen or fraudulently used, contact the **State of New Jersey Motor Vehicle Commission** at **1-609-292-6500** or visit **www.state.nj.us/mvc/license/liclost.htm**.

Regularly monitor your driving history.
Visit: **www.state.nj.us/mvc/license/driverhist.htm**.

Steps to take to protect yourself from Identity Theft

- **Protect your personal information**, especially your Social Security Number.

- **Carefully review** your bank and credit card statements regularly for inaccuracies. If you see a charge you don't recognize, large or small, contact your bank or credit card company. The telephone number is typically located on the back of the card.

- **Report lost or stolen identification cards**, such as your Social Security card, Medicare card, insurance card or driver's license, to the issuing agency immediately.

- **Report lost or stolen debit or credit cards** to the issuing company as soon as you notice it is missing.

- **Secure** all documents that contain sensitive personal information, such as bank or credit card statements, benefits statements and medical records.

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

- **Empty your wallet** or purse of extra credit cards or IDs (Social Security card, birth certificate, passport) and cut up cards that are not in use.

- **Do not keep ANY personal information** (such as Social Security numbers, bank account numbers, passwords or PINS) on anything in your wallet or purse.

- **NEVER** discard personal information in the trash. Instead, **SHRED** all documents containing personal or financial information, including pre-approved credit card and loan applications.

Steps to take to protect yourself from Identity Theft *(continued)*

- **Opt out of receiving credit card offers** by contacting the Federal Trade Commission (FTC) at **1-888-5-OPT-OUT** (1-888-567-8688) or online at: **www.optoutprescreen.com**.
- **NEVER** provide **ANY** personal information, including credit card numbers, bank account information or your Social Security Number over the telephone, unless you have a trusted business relationship with the company and **YOU** have initiated the call.
- **Monitor your credit regularly** by ordering a copy of your credit report every year from all of the major credit reporting agencies to check for fraudulent activity or discrepancies. In New Jersey, you can obtain one free report every 12 months from each of the credit reporting agencies. *See page 35 for further information regarding the credit reporting bureaus.*
- **Use any extra security measures** offered by your financial institutions, such as two-factor authentication and login alerts.

- **Monitor data breach announcements** to see if you are an affected consumer.
- **Be safe when online** and limit the amount of personal information you post and share online.
- **Always use strong, unique passwords** for all online accounts and change them regularly. Consider using a password management service.
- **Do not use public wi-fi** to make purchases or login to your email or mobile banking site.
- **Do not click or open unknown links or attachments**. Scammers will often send emails and texts aimed at tricking the recipient to click on a link or open attachments. This is referred to as "phishing." Government agencies and legitimate businesses will not request personal information via email, text or phone call.

Steps to take to protect yourself from Identity Theft *(continued)*

- **Check your internet/web browser privacy policy** and fine-tune your security settings. Keep your operating system, browser, and other software up-to-date.
- **Install virus protection and firewall software** on your computer and always make sure they are up-to-date.
- **Download only those applications** you plan to use and check the privacy policies and permission of the applications before you download an app.
- **Enable security functions on your phone and computer**—especially if you have stored passwords or apps that link to your financial institutions. For example, use a fingerprint or password to lock your phone.
- **When disposing of digital devices** such as phones, computers and tablets, make sure to completely erase all of your data — this includes modern copiers which may have an internal hard drive. If in doubt, destroy the devices.

- **Communicate with the elderly and young people in your family about the dangers of Identity Theft.** Teach them to be vigilant in their everyday transactions involving money and personal information, as well as in their online activity and social media presence.

- **When using social media**, use discretion as to disclosure of personal details about yourself, your family and friends. For example, do not reveal exact birthdates, vacation plans, health issues or family history.

For additional information about Identity Theft, visit:
www.njsp.org/tech/identity.html.

If you suspect that your identity has been stolen, report it to the appropriate authorities listed below

When to contact your local police department:
If you suspect that you may be a victim of Identity Theft, immediately file a report with the local police department. Once your police report has been filed, request a copy to send to credit reporting agencies and creditors if you decide to contest suspicious charges. *Note: According to N.J.A.C. 2C:21-17.6, the local law enforcement agency is required to take your complaint and provide you with a copy.*

When to contact your financial institutions:
Contact fraud departments of all of your credit card companies, creditors, banks and financial institutions (including mortgage and student loan companies) to alert them and request replacement cards.

Contact the national credit bureaus to request a copy of your credit report. You can also request to have a credit freeze or fraud alert placed on your credit report free of charge. A security freeze, also known as a credit freeze, restricts access to a consumer's credit file, making it harder for identity thieves to open new accounts in the consumer's name. A fraud alert tells businesses to check with the consumer before opening a new account.

- Equifax: **www.Equifax.com/personal/** or **1-800-685-1111**
- Experian: **www.Experian.com/** or **1-888-397-3742**
- Transunion: **www.TransUnion.com/credit-help** or **1-888-909-8872**
- Innovis: **www.Innovis.com** or **1-800-540-2505**

*Note: As a resident of New Jersey, you have the right to obtain a **FREE** copy of your credit report every 12 months from* **www.annualcreditreport.com**.

If you suspect that your identity has been stolen, report it to the appropriate authorities listed below *(continued)*

When to contact the U.S. Federal Trade Commission:
Contact the Federal Trade Commission at **www.identitytheft.gov/** to create an Identity Theft Report and a recovery plan. You may need these later when dealing with some of the affected agencies.

When to contact the U.S. Social Security Administration:
If you believe that your Social Security card has been lost or stolen, or believe that your Social Security Number has been misused, contact the Social Security Administration at **1-800-269-0271**, or **https://www.oig.ssa.gov/report**.

When to contact the New Jersey Motor Vehicle Commission:
If you suspect that your driver's license or registration was lost, stolen or fraudulently used, contact the New Jersey Motor Vehicle Commission at

1-609-292-6500 or **www.njmvc.gov**. *Note: You may have to appear in person at a regional office to fill out an ID Theft Affidavit.* You will be required to bring forms of identification and all proof of fraudulent activity.

When to contact the U.S. Department of State:
Protect yourself from passport fraud–contact the U.S. State Department at **www.travel.state.gov/content/travel/en/contact-us/reporting-fraud.html**, **1-877-487-2778**, or **PassportVisaFraud@state.gov** to alert the Department that you were the victim of identity theft. Request an alert if anyone attempts to use your identity to acquire a passport.

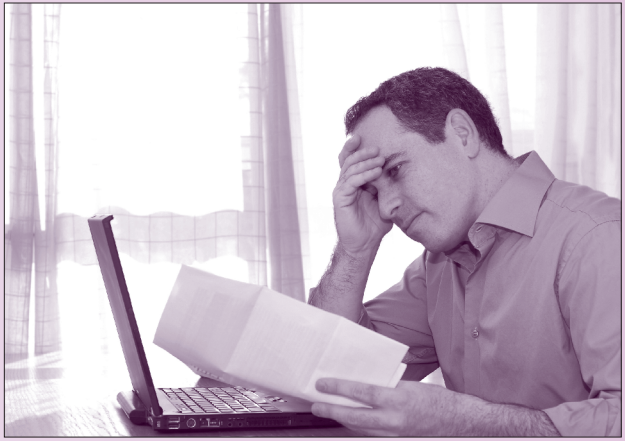
When to contact the U.S. Postal Inspection Service:
If you suspect that your address has been changed without your permission, notify your local U.S. Postal Inspector to find out what your address was changed to and instruct them to forward all mail addressed to you to your correct address. Contact the U.S. Postal Inspectors at **1-877-876-2455** or **www.uspis.gov/report**.

If you suspect that your identity has been stolen, report it to the appropriate authorities listed below *(continued)*

When to contact the U.S. Department of Education:
If you believe you are the victim of student loan Identity Theft, contact the U.S. Department of Education Office of the Inspector General hotline at **1-800-647-8733** and/or the Federal Student Aid Ombudsman Group at the U.S. Department of Education at **1-877-557-2575**.

Maintain a thorough record of the Identity Theft incident

- Keep a complete set of records, including a log with notes of all telephone conversations with credit reporting bureaus, creditors and/or debt collection agencies (date/time/name).
- Keep copies of all paper or electronic correspondence you send and receive related to the Identity Theft incident.
- Keep a record of the time spent and any expenses you incurred.
- When sending supporting documents, send copies, not originals.
- Be aware of all deadlines.
- Send letters by certified mail, return receipt requested.



Identity Theft Handbook

www.NJConsumerAffairs.gov ■ 1-800-242-5846