LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

JUNE 2025

IDENTITY THEFT PROTECTION

What is Identity Theft?

Identity theft happens when someone wrongfully obtains and uses another person's personal or financial information without their permission for financial gain. This information can include:

- Names and addresses
- Credit card or Social Security numbers
- Bank account numbers
- Medical insurance account numbers

You may not know that you experienced ID theft immediately. Beware of these warning signs:

- Bills for items you did not buy
- Debt collection calls for accounts you did not open
- Information on your credit report for accounts you did not open
- Denials of loan applications
- Mail stops coming to or is missing from your mailbox

Adversaries take your information and will create or active new accounts, use your existing accounts, or obtain medical services. Identity theft can have serious consequences for you and your family. It can negatively affect your credit, it can get you sued for debts that are not yours, result in incorrect and potentially health-threatening information being added to your medical records and may even get you arrested.

How Identity Theft Happens?

Identity theft happens when someone unlawfully obtains and uses your personal information—like your name, Social Security number, credit card details, or bank account information, typically for financial gain. It can happen in a variety of ways, both online and offline.

Adversaries will gain access to your identification through the following:

- Steal wallets or purses in order to obtain identification, credit and bank cards.
- Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details.
- Fill out change-of-address forms to forward mail, which generally contains personal and financial information.
- Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit.
- Obtain personnel records from a victim's place of employment.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

- "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip.
- Swipe personal information that has been shared on unsecured websites or public Wi-Fi
- Steal electronic records through a data breach.
- "Phish" for electronic information with phony emails, text messages and websites that are solely designed to steal sensitive information.
- Pose as a home buyer during open houses in order to gain access to sensitive information casually stored in unlocked drawers.

How Can You Recognize Identity Theft?

Look closely for charges or withdrawals you did not make. Even a small charge or withdrawal can be a danger sign. Thieves sometimes will take a small amount from your checking account and then return to take much more if the small debit goes unnoticed. Review your free credit reports from each of the three major credit bureaus. If an identity thief is opening financial accounts in your name, these accounts may show up on your credit report. Look for:

- Inquiries from companies you've never contacted
- Accounts you didn't open
- Wrong amounts on your accounts

What Should I Do If My Identity Is Stolen? Report it immediately!!!

Visit **IdentityTheft.gov** to report identity theft to the FTC and get a personal recovery plan. **IdentityTheft.gov** walks you through recovery steps for more than 30 types of identity theft.

You can also use **LifeLock**, a comprehensive identity theft protection service designed to safeguard your personal information across various platforms, including credit, banking, and online activities. LifeLock offers proactive monitoring, real-time alerts, and dedicated restoration support to help you maintain control over your identity.