'Identity Theft Knowledge' – Guard, Protect, and Take Back your Life. FREE report'

By

Lee Rupprecht

Identity Theft Explained

Identity Theft occurs when your personal information is taken and used without your knowledge. It is a serious crime and should not be underestimated or overlooked. A person whose identity has been stolen can spend years and hundreds of dollars repairing the damage done to their name and credit. In the blink of an eye your life can be turned upside down by identity theft; loss of job opportunities, loans denied, negative credit ratings, and in rare cases, arrested for crimes you did not commit.

How Your Identity Gets Stolen

Millions of people have their identity stolen every year. It usually starts with the misuse of your personal information; name, social security number, credit cards, and financial account information. A thief will use this knowledge to gain more information about you and get everything they can before moving on.

There are a variety of ways in which to acquire your personal information.
1. Dumpster Diving
2. Skimming
3. Phishing
4. Address Change
5. Stealing
6. Pre-texting

Dumpster Diving:
They look through your trash for bills, financial statements, or anything else that can be used to assume your identity. Your car or home may also be broken into to find your personal information, including passwords to your computer.

Skimming:
Your credit card or debit card numbers are captured by a special storage device, which can be attached to the swipe-capture machine in a store, or placed on an ATM. Another device can be secretly attached to any computer and record every keystroke entered.

Phishing:
Thieves pretend to be online legitimate financial institutions or organizations. They will send you spam, letters of concern, or pop up messages to get you to reveal your personal information.

Address Change:
Thieves may complete a "change of address form" to divert your mail to another location.

Stealing:
Thieves will do whatever it takes to get your personal information. They may steal your wallet or purse, your mail, bank or credit card statements, new checks, tax information, abuse their employee authorization, watch as you input your account number or pin number in an ATM and other machines, memorize your account numbers as you write a check, and fill out pre-approved credit offers. They may also steal your personnel records, electronically transfer your information, or bribe someone with legal access to your reports.

Pre-texting:
Thieves may use false pretenses to get your information from financial institutions, telephone companies, and other sources. They may pose as an

authority figure, a research firm, or other organization to collect information about you such as name, address, birth date, and social security number. After obtaining the information they need, they call your financial institution and pretend to be you or someone with authorized access to your account. They may claim they forgot their checkbook and need information about their account using your information. With this information, they may gain other personal information about you such as your bank and credit card account numbers, your credit report information, and the status of savings and investment portfolios.

Some information about you may be on public record such as whether you own a home, pay your taxes, or have ever filed bankruptcy. It is not pre-texting for another person to collect this kind of information.

Law:

The Law states it is illegal for anyone to:

- Use false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious, or fraudulent statements or using false, fictitious, or fraudulent documents, or forged, counterfeit, lost, or stolen documents.

What Thieves Do With Your Information

Thieves have a variety of ways to use your personal information.

Credit Card Fraud:

- New Accounts can be opened in your name and the delinquent accounts appear on your credit reports when they don't pay the bills.
- Change the billing address on your credit cards to a new location, then charging up as much as they can on your cards. The bills would be going to the new address and not being paid. It could take some time before you realize there was a problem.

Phone & Utility Fraud:

- New Phone or Wireless accounts opened in your name, or a large amount of charges on your existing account.
- Your name may be used to get utility services such as electricity, heating, or cable TV.

Bank & Finance Fraud:

- Counterfeit Checks can be created using your name or account number.
- New bank account can be opened in your name and bad checks written.
- Your ATM or Debit Card could be cloned. They could make electronic withdrawals in your name and drain your accounts.
- Loans can be taken out in your name.

Government Documents Fraud:

- A driver's license or official ID card can be issued in your name, but with their picture.
- Government Benefits could be obtained using your name and Social Security Number.
- A fraudulent tax return could be filed using your information.

Additional Fraud:

- They may get a job using your Social Security Number.
- Rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. When they don't show up for their court date, a warrant for arrest is issued in your name.
- File for bankruptcy under your name to avoid paying debts they have incurred under your name, or to avoid eviction.

How to Detect Identity Theft

Monitor your accounts and bank statements continuously each month, and check your credit report on a regular basis.

Identity Theft Signs to look for:

- Accounts you didn't open and debts on your accounts you can't explain.
- Fraudulent or inaccurate information on your credit reports, including accounts and personal information, such as your Social Security Number, address(es), name or initials, employers.
- Failing to receive bills or mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover their tracks.
- Receiving credit cards you didn't apply for.
- Being denied credit, or being offered less favorable credit terms, such as high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses regarding merchandise or services you didn't buy.

What to Do if Your Identity is Lost or Stolen

Quickly perform the following steps if your personal information has been lost or stolen. It may reduce the risk of an identity thief.

- Financial: Immediately close your accounts, such as credit cards and bank accounts. Place passwords on new accounts you open. Do not use your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, or a series of consecutive numbers. An identity thief may know this information or your usual habits of making passwords. Be spontaneous.
- Social Security Number: Call the toll-free number of any of the nationwide consumer reporting companies and place an initial fraud alert on your credit reports. An alert can help stop someone from opening new credit accounts in your name.
- Driver's License & other government issued ID: Contact the agency that issued your license or government ID, cancel the document, and get a replacement. Each agency may have their own procedures which you follow. Ask the agency to flag your file to prevent anyone else getting a license or ID documentation in your name.
- Afterwards: After doing the above steps, closely watch for signs that your information is being misused.

Identity Theft Victim

Complete the following four steps as soon as possible, and keep a detailed record or your conversations and copies of all correspondence for your protection.

1. Place a Fraud Alert on your credit reports and review them carefully.

A fraud alert can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of one of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their reports too.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you are entitled to order one free copy of your credit report from each of the three consumer reporting companies and, if you ask, only the last four digits of your social security number will appear on your credit reports. This will help safe guard your social security number from others looking at your reports.

Once you get your reports, look them over carefully. Search for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you can not explain. Check all your information including your name or initial, address(es), social security number, and employers. Make sure everything is correct. If you find fraudulent or inaccurate information, get it removed.

Continue to check your credit reports periodically, especially for the first year after you discover the identity thief, to make sure no new fraudulent activity has occurred.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Always follow up in writing, and include copies (NOT originals) of supporting documents. It is important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep an organized file of your correspondence and enclosures.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

3. File a complaint with the Federal Trade Commission.

You can file a complaint with the federal trade commission using the FTC's Identity Theft Hotline, toll-free; 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victim's complaints to other government agencies and companies for further action, as well as investigate companies for violation of laws the agency enforces.

4. File a local police report or with the police in the community where the identity theft took place.

Call your local police department and tell them you want to file a report about your identity theft. Ask them if you can file the report in person. If you can not, ask if you can file a report over the Internet or telephone.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, such as your state police. You can also check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the blue pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

Always ask for a copy of the police report and keep them with the rest of your files.

Lasting Effects of Identity Theft

Predicting how long the effects of identity theft will last is difficult to measure, for each case is different. There are many factors involved including the type of theft, whether the thief sold or passed your personal information to other thieves, whether the thief is caught, and problems related to correcting your credit report.

If you are a victim of identity theft, you should monitor your financial records for several months after the crime is discovered, review your credit reports once every three months in the first year of the theft, and once a year thereafter. Keep a constant look out for signs of identity theft.

Never delay in correcting your records and contacting all the companies that opened fraudulent accounts. Make the initial contact by telephone, and follow it up in writing. Keep copies of everything in an organized file system. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

Dealing with problems resulting with identity theft can be time consuming and frustrating. Be assertive, organized, and knowledgeable about your legal rights. Some laws require you to notify companies within specific time

periods. Do not delay in contacting any companies to deal with these problems, and ask for supervisors if you need more help than you are getting.

Minimize Further Identity Theft

There will always be some risk, but there are certain steps you can take to minimize recurrences.

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information such as your mother's maiden name, your birth date, last four digits of Social Security Number, or a consecutive series of numbers. When opening new accounts ask to use a password instead of using mother's maiden name (many businesses still ask for mother's maiden name on their applications).
- Make sure your personal information is in a secure location (safe, lock box, safety deposit box, etc) especially if you have roommates, employ outside help, or are having work done in your home.
- Contact, in person if possible, all the places and businesses that collect your personal identifying information and ask about information security procedures; work place, businesses, doctors offices, dentist offices, etc. Find out who has access to your personal information and verify that it is handled securely. Ask about disposal procedures for those records. Find out if your information will be shared with anyone else and how your information can be kept confidential if it is shared.
- Do not give out personal information on the phone, through the mail, or on the Internet unless you have initiated the contact or are sure you know who you are dealing with. Remember, identity thieves may pose as anyone to get your information.
- Shred unwanted mail and trash completely before putting it in the trash can.
- Do not carry your Social Security Number; leave it in a secure place.
- Give your social security number when absolutely necessary. You can ask to substitute another number for your SSN if they are using it for a policy or record keeping file.
- Carry only the identification information and the credit and debit cards that you will actually need when you go out. Keep the rest in a secure location.

- Be cautious when responding to promotions; they could be phony promotional offers used to get your personal information by thieves.
- Keep your wallet and purse in a safe place at work.
- Keep copies of administration forms with your sensitive information in a safe place.
- When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.
- Computer Security:
  1. Use a secure browser
  2. Virus protection software
  3. Install firewalls
  4. Do not open files sent to you by strangers
  5. Try not to store financial information on laptop unless absolutely necessary (use a strong password with a combination of letters and numbers both upper and lower case)
  6. Wipe hard drive and delete all personal information before disposing of computer.

Ways to Fight Identity Theft

Awareness is a powerful tool against many forms of identity theft. Learn about identity theft and educate others. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

An identity thief's job becomes much harder when you are armed with the knowledge of how to protect yourself and take action. Help fight against Identity Theft by educating your family, friends, neighbors, and members of your community. Internet Filtering can help protect children from on-line dangers. Periodically clean your computer system eliminating unnecessary information and check for errors.