Section 2 - Identity Theft

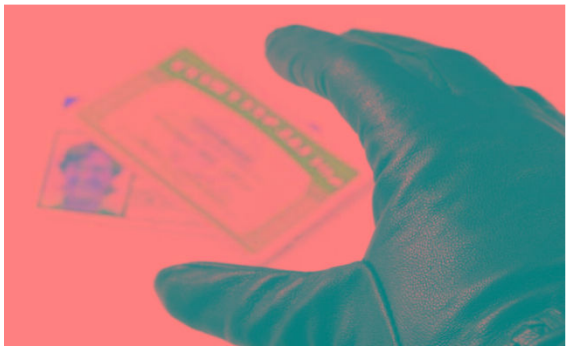
Introduction

Identity theft is one of the fastest growing crimes in the world today and can be one of the most costly problems consumers face. Consumers receive offers almost every day that sound too good to be true. Most of those offers used to come through the mail or by telephone, but today, they also come through email and the Internet. Scam artists have no national boundaries and may, in fact, be located in other countries but “doing business” in the United States.

What is Identity Theft?

Identity theft means that someone uses your personal information (your name, social security number, credit card number or other similar pieces of information) without your permission. Generally, people who steal your identity use this information to rent an apartment, get a cell phone, get another credit card, or take other actions in YOUR name. Of course, they get to use whatever they have illegally purchased, and you get the bills.

According to the Federal Trade Commission, about 9 million people in the United States alone have their identities stolen each year. You may know someone who has been a victim. It can take hundreds of dollars and many hours of your time to correct the problem. Meanwhile, your credit history and your reputation suffer. You may even fail to get a job, rent an apartment, or be denied a loan or scholarship because of the negative information gathered about you, even if you had nothing to do with the problem. Some victims have even been arrested for a crime because someone else used their names.



How Do They Do It?

ID thieves use several different approaches to get information about you. These include:

Dumpster Diving and mailboxes. They rummage through your trash looking for bills or other paper with your personal information on it. They may ift items from your mailbox (bank statements, credit card statements, preapproved credit offers, new checks, or tax information

Skimming. They steal credit card or debit card numbers with a special device when processing your card.

Phishing. They pretend to be banks, the IRS or some other organization and send you an email or a letter (or even make a phone call) asking for personal information. They may also duplicate credible websites to gain that information.

Changing Your Address. They complete a change of address card, creating a new address for you so they can receive your billing statements. Once they have the statements, they can access your account.

Stealing. They steal billfolds, purses, smartphones and other portable tech devices.

Hacking. They may hack into your computer or another computer system, including schools, credit card companies, and other places maintaining personal information.

Unfortunately, someone may use your personal information for months before you find out. Imagine the bills and fees that can accumulate against you before you know about it.

How Do You Know It Has Happened?

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.
- 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.

How to Protect Yourself from ID Theft

Unfortunately, you cannot completely protect yourself from being a victim, but there are several things you can do to minimize the potential.

- Use passwords on your credit card, bank and cell phone accounts. Avoid passwords that are information others may know or any part of your birth date, address, Social Security number or phone numbers. Use passwords that are a combination of letters and numbers and change them often.

- Put your personal information in a secure place, such as a small safe or lock box, to prevent easy access to it. Carry only the identification information and the credit/debit cards that you actually need when you go out.

- Shred all papers with your personal information before throwing them in the trash. Be sure to shred credit card offers, credit card checks mailed from your card company, insurance forms, and other papers with your name and personal information on it.

- NEVER give out any personal information on the phone, through the mail, on the Internet, in an email, or in person unless you have initiated the contact and you are sure who you are dealing with. Remember, the IRS, your bank,

your credit card company, and other places where you do business do not need to ask you for that info!

- Avoid cutting and pasting or clicking Web links from emails, unless you are certain it is a valid link.Only enter personal data on secure websites.
- Place your outgoing U.S. mail in a postal mail drop or take it to the post office instead of putting it in the mailbox of your house. Anyone can come by and get it. If you are leaving home overnight, have the post office hold your mail until you return.
- Take care with promotions or charitable organizations. Research them to confirm that they are reputable and legal..
- Order a copy of your credit report from the three primary credit bureaus to monitor your credit history. You are allowed three each year at no cost. Many financial vendors you already deal with will also provide you your credit reporting info as part of their services.

Steps to Take if Victimized

- File a complaint with the Federal Trade Commission. Their Web site is www.ftc.gov and contains phone numbers, forms, and general information.
- Contact the fraud division of the three credit bureaus and ask them to put a fraud alert on your credit files. If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. Once the information is blocked, it won't show up on your credit report, and companies can't try to collect the debt from you. If you have an FTC Identity Theft Report, credit bureaus must honor your request to block this information
    - o Equifax 1-800-525-6285 www.equifax.com
    - o Experian 1-888-397-3742 www.experian.com
    - o TransUnion 1-800-680-7289 www.transunion.com
- Contact your local police or the police in the city where the identity theft took place.
- Contact your financial institutions, credit providers or service accounts

to verify that they haven't been affected. Close fraudulent accounts opened in your name. Order a free copy of your ChexSystems report, which compiles information about your checking accounts. To get your report, contact ChexSystems at 1-800-428-9623.

- Call the fraud department of each business where an account was opened or has had fraudulent activity. Provide a copy of the complaint filed with the police department and the FTC for validation.
- **Review your bill payment process** You may need to reset any payment options you have in place if you need to lock or close accounts. If the fraud causes a major interruption in your cash flow you may need to reach out to debtors to discuss options for delayed payments..

Protect Your Future

- **Review your money management and bill payment process** Gaps or weaknesses in how you manage your money and accounts are often how your identity or information is stolen.
- **Improve your Personal Fraud Protection Plan** Figure out how the fraud occurred and change your behavior around that.
- **HAVE AN EMERGENCY FUND** you may need to access it to cover the disruption and give you time to reset things.

Lesson Review

Match the following terms to the scenarios. Place the letter of the correct term in the blank in front of the scenario.

A. Changing your address B. Skimming C. Stealing D. Hacking

E. Phishing F. Pretexting G. Dumpster Diving

___1. John throws all of the copies of his bills and credit card statements in the trash. He receives a call from his credit card company asking him if he has been to Cancun recently and purchased a large amount of diving equipment. John has never traveled outside of the United States. Which term describes how a thief got John's credit card information?

___2. Kaden received an email asking him to confirm his credit card information and then he clicked on the link in the email that directed him to a site that asked him to fill in the blanks with his name, social security number and his credit card number. The site looked like the legitimate organization's site so he complied with the request. Soon after he supplied the information, he received a bill from his credit card company with several purchases he had not made. Which term describes what happened to Kaden?

___3. Mary's grandmother paid for their lunch with a credit card. The waitperson brought her back the card and she signed the receipt. A month later, several charges appeared on her grandmother's credit card bill that she had not made. What term describes what the waitperson did?

___4. Kurt is a computer nerd with exceptional skills. He is able to access computers that belong to other people. He obtains Mr. Ling's bank and credit card account numbers and uses them to order items from Amazon.com. What term describes what Kurt is doing?