Identity Theft

by Sophia

WHAT'S COVERED

In this lesson, you will learn how to protect yourself from identity theft and what to do if your information has been compromised. You will explore how technology can help keep you safe. Specifically, this lesson will cover:

WATCH

Are you interested in a video preview of this lesson? Click play on the following video and **fast forward it to 4:30** to investigate the ways that criminals could steal your financial identity. When you're through, move on to section 1.

1. Identity Theft

Let's now turn our attention to identity theft. The U.S. Justice Department defines **identity theft** as a crime in which someone wrongfully obtains and uses your personal data in some way that involves fraud or deception for his or her economic gain. The following illustration shows the most common forms of identity theft.

Before 1998, identity theft was not considered to be a federal crime. This changed when news spread that a

convicted felon had done the following:

- Stolen the identity of a man and ran up more than $100,000 in credit card debt.
- Obtained a mortgage for a new home.
- Purchased cars, boats, motorcycles, and guns in the man's name.

Worse still, the thief repeatedly called the man and his wife to taunt them. Although the thief was eventually caught, he only spent a short amount of time in jail for misrepresenting himself for the purchase of a gun. He never paid back the money he stole, nor did he spend a day in jail because of his theft!

Technology: Skill Tip

Consider using your technology skill to set up two-step authentication for banking or social media. This adds a second code to your password to confirm your login and identity.

TERM TO KNOW

Identity Theft

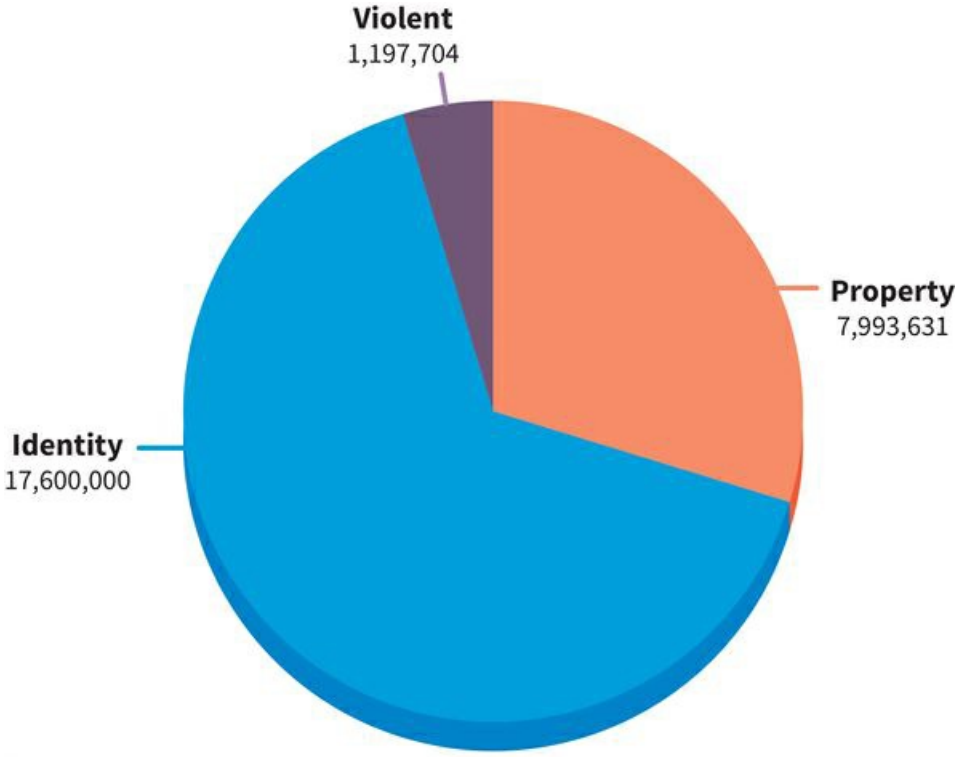
A crime in which someone wrongfully obtains and uses your personal data, such as your name and Social Security number, in some way that involves fraud or deception for his or her economic gain.

1a. The Facts of Identity Theft

Fortunately, state and federal laws now recognize identity theft as a crime. However, just because identity theft is illegal does not mean that the occurrence of identity theft has declined. In fact, the opposite is true. Consider the following statistics from the U.S. Department of Justice:

- Nearly 18 million households have had at least one person age 12 or older experience identity theft.
- More than 35% of all households in the United States have experienced misuse or theft from a bank, savings, or utility account (e.g., electricity or water).
- The total loss associated with identity theft exceeds $13 billion per year.

As shown in the pie chart below, the number of identity thefts in the United States is greater than the number of reported violent and property crimes combined!



Source: Department of Justice (2015).

The really bad news is that law enforcement agencies are not equipped to help most people who experience identity theft. Usually, the amount stolen is considered too low, or it is nearly impossible to find the thief.

How does identity theft happen? Thieves can steal your identity in a number of ways:

- Stealing your wallet or purse.
- Going through your garbage looking for receipts and credit card offers.
- Hacking into your credit card or bank account.

Sometimes, people innocently give thieves their account numbers and passwords by responding to bogus e-mails or phone calls.

1b. Protecting Yourself from Identity Theft

It is up to you to protect yourself from being an identity theft victim. Here is what the**Federal Bureau of Investigation (FBI)** recommends to avoid being an identity theft victim.

- Never throw away ATM receipts, credit statements, credit cards, or bank statements; always shred or destroy these documents.
- Never (ever) give your credit card number over the telephone unless you made the call.
- Do not respond (ever) to a **phishing scheme** – an unsolicited e-mail asking you to provide personal information (such as your Social Security number) or confirm the details of a credit account. You will know if someone is attempting a phishing scheme if you receive any e-mail with a statement such as the ones shown in the sample emails below.
- Always reconcile your bank accounts monthly and report any problems to your bank or creditor immediately. Further, keep a list of all your credit cards, debit cards, and each account's contact information somewhere secure, such as a safe deposit box.
- Obtain a copy of your credit report annually and report anything unusual right away.

Sample Phishing E-mails

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

You should also take preemptive action by doing a**credit freeze**. Freezing your credit seals your credit reports so that no new accounts can be opened unless you unfreeze the account using a personal identification number (PIN).

HINT

Freezing your accounts will not negatively affect your credit score, and the small fee charged by the credit bureaus (about $3 to $15) is well worth the cost.

If you suspect that you have been a victim of identity theft, take the following steps.

STEP BY STEP

1. Contact your local police or sheriff department.
2. Alert your credit card company or financial institution.
3. Check with your insurance agent. Some homeowner's and renter's insurance policies include coverage for a stolen identity or financial frauds.

As you progress in your lifetime financial journey, it is important to keep an eye out for people and organizations that intend to push you off-track. Frauds and rip-offs, for the most part, can be avoided. Being diligent in protecting your identity and cautious with your financial records is a good way to stay focused on reaching your long-term financial goals.

Technology: Skill Tip

Consider using messaging accounts (like WhatsApp and Signal) that utilize encryption, or a secret coding, to keep the content of your messages hidden from anyone else except the individuals sending and receiving them.

IN CONTEXT

Zoe, your friend from class, is a full-time student who also works 20 to 30 hours per week to pay as much of her schooling costs as possible. She then takes out student loans to cover the remaining expenses. Zoe recently received a phone call informing her that she has been selected for a student loan forgiveness program. Zoe tells you that she is so excited because the person on the phone told her that she would only need to pay a one-time enrollment fee of $999. After that, Zoe would simply

need to fax her transcript, with her Social Security number, and her student loan balance would be reduced by $2,500 for every A that she received going forward. Zoe is so excited because she is a good student and this will give her some extra motivation to get straight A's. *What should you tell Zoe?*

Here's the solution:

This sounds like a definite scam. Before Zoe sends any money or gives out her personal information, she should ask to receive written material about the company and this program and the phone number she can use to call them back. Zoe should also then check the company's rating with the **Better Business Bureau** or **Chamber of Commerce**, or investigate the company using an Internet search.

Typically, scammers won't give you time to think about the decision, so for Zoe it might be too late if she already gave them her credit card or other information over the phone to sign up. Legitimate companies will give you time to think about it and call them back on a number that you request. Regardless, Zoe should immediately notify the authorities if she discovers that this is a scam.

TERMS TO KNOW

Phishing Scheme

An unsolicited e-mail asking you to provide personal information (such as your social security number) or confirm the details of a credit account.

Credit Freeze

Allows your credit reports to be sealed so that no new accounts can be opened unless you unfreeze the account using a personal identification number (PIN).

SUMMARY

In this lesson, you learned how to **protect yourself from identity theft**. For example, never give credit card information out over the phone unless you made the call. And never throw your bank receipts into the trash. Strong technology skills can also help in this effort. **One fact about identity theft** is that in the U.S., the number of **identity thefts** exceeds property and violent crimes combined! If you find that you've been victimized, the first steps are freezing your credit and contacting your local police or sheriff's department. Then be sure to notify your financial institutions and credit card companies of the breach.

ATTRIBUTIONS

- Crime in the United States (2015) | **Author:** U.S. Department of Justice | **License:** Public Domain

TERMS TO KNOW

Credit Freeze

Allows your credit reports to be sealed so that no new accounts can be opened unless you unfreeze the account using a personal identification number (PIN).

Identity Theft

A crime in which someone wrongfully obtains and uses your personal data, such as your name and Social Security number, in some way that involves fraud or deception for his or her economic gain.

Phishing Scheme

An unsolicited e-mail asking you to provide personal information (such as your social security number) or confirm the details of a credit account.