



UNIT 3-4

Preventing Identity Theft

Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. The perpetrator may use your personal information such as your name, social security number, or credit card number to commit crimes. The most common identity theft complaints are credit card fraud, followed by utility or phone fraud; bank fraud; employment-related fraud; government document or benefit fraud and loan fraud. The identity thieves may rent an apartment in their victim's name, obtain a credit card, or establish other lines of credit in the victim's name such as a telephone account, store credit account, or a checking account. Identity thieves have even begun targeting infants for identity theft. Often the theft is not discovered until the child is a teenager or applying for his or her first line of credit.

The number of victims of identity theft has increased dramatically over the past several years. The Federal Trade Commission estimates that as many as 9 million Americans have their identity stolen in a given year. Nationally, that equals 24,657 per day, 1,028 per hour, or 17 per minute! In 2006, Kentucky ranked 44th nationally in identity thefts with 1,766 complaints filed. This is 42.0 complaints per 100,000 people in the state.

Identity theft is the number one complaint received by the Federal Trade Commission—42% of all fraud complaints received. Victims of identity theft spend an average of \$1,400 in out-of-pocket expenses, an increase of 85% over the past 7 years. It is estimated that the business community loses between \$40,000 and \$92,000 per instance of ID theft in fraudulent charges.

What are the steps you should take to reduce your chances of becoming a victim of identity theft?

Case Study Application

The case study application is designed to illustrate some of the key points made in the text.



CASE STUDY: ANDREW LEARNS ABOUT IDENTITY THEFT

Andrew has begun developing his credit history. He opened checking and savings accounts and a retail credit account that he has been paying on time. He also opened a cellular telephone account to build his credit record. Andrew has continued his employment at the local pizzeria for quite some time. He charges a minimal amount to the credit card each month and pays the balance in full each month. He is currently living within his means.

Now that he is beginning to establish his credit in order to further his ability to become a future homeowner, he has begun to worry about protecting himself against the pitfalls of identity theft. One of his coworkers at the pizzeria recently received letters that her charge accounts were overdue. She noticed that they were from companies where she never made purchases. After further investigation, the purchases were for items she didn't buy. Andrew wonders if he could fall victim to a similar situation.

What Is Identity Theft

Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. This could include using your name, your social security number, your credit card number, opening a credit account in your name or other crimes. With an average of one out of every four Americans having their identity stolen, chances are you may know someone who has had their identity stolen.

How can your identity be stolen? There are many ways that thieves use to steal someone's identity. This can include dumpster diving. This is when thieves look through trash for bills or other papers with personal information on it. They also use phishing. The thieves pretend to be financial institutions and send pop-up messages or spam to get you to reveal your personal information.

Another method used is to change your mailing address. They will divert your billing statements to another address and then assume your account. Identity thieves also use plain old-fashioned stealing to commit identity theft. They steal wallets, purses, mail, credit card statements, pre-approved credit offers, new checks, or even tax information. They may even bribe employees who have access to your financial information.

Finally, identity thieves may use false pretenses for obtaining your personal information. They use a variety of tactics to access your personal information. For example, they may call you claiming to be a research firm or your financial institution. Then, they will ask for your name, address, birth date, and social



security number. With this information, the thief has everything she or he needs to use your personal information to fraudulently open accounts or even to access your accounts!

What do identity thieves do with your personal information once they have acquired it? There are many different ways that identity thieves may use your personal information. This could include government documents fraud. The thief may get a driver's license or office identification card with your name, but their picture. They may file a fraudulent tax return, or they may use your name and Social Security number to obtain government benefits. They may even give your information to a law enforcement officer upon an arrest. If they fail to appear for the assigned court date, a warrant will then be issued for arrest in your name!

Another type of fraud committed by identity thieves is bank or finance fraud. They may open a bank or checking account in your name and write bad checks. They may take out a loan in your name or create counterfeit checks using your name or actual account number. Identity thieves also use your personal information to commit phone or utility fraud. They can use the information to open a new phone or wireless account in your name. They may even use your identity to get utility services such as cable television or electricity.

Finally, identity thieves may use your personal information to commit credit card fraud. They might change the billing address on your credit card and then run up charges on your account. They might open a new credit card account using your name. Then they use the cards and don't pay the bills. The delinquent accounts will be listed on your credit report.

- Analyze the different ways that identity thieves are able to access their victim's personal information. What steps can consumers take to avoid this access?

How Can You Find Out If Your Identity Has Been Stolen

Identity theft is a federal crime that takes place when someone "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." A name or Social Security number is a means of identification as are credit card numbers, cellular telephone serial numbers, or any other piece of information that may be used alone or in conjunction with other information to identify a specific person.

The best way to find out if your identity has been stolen is to monitor your accounts each month and check your credit report regularly. Many victims of identity theft find out that their identity has been stolen after a good deal of damage has been done. Victims may find out when a collection agency contact them for collection of overdue debts the victim never incurred. They may find out when they



apply for a mortgage or for other credit and find out that their credit history is preventing them from acquiring the loan. Victims may even find out when they receive something in the mail that they did not initiate. For example, a job they never had, an apartment they never rented, or a house they never bought. In very rare cases, some victims of identity theft have even found out about the theft when they were served with an arrest warrant for a crime they didn't commit!

If your identity is stolen, take steps quickly to minimize the impact. File a police report, notify your creditors. Close credit and bank accounts immediately. When opening new accounts, place security passwords on them. Avoid using obvious passwords (your mother's maiden name, your birthday, children's names, or a series of consecutive numbers).

Next, call the three nationwide consumer reporting companies and place a fraud alert on your credit reports (Equifax: 1-800-525-6285; Experian: 1-888-397-3742; and TransUnion: 1-800-680-7289). This alert will prevent someone from opening new accounts in your name. It is a signal to warn creditors that they must verify your identity before they issue credit in your name. There are two types of fraud alerts—initial and extended. An initial alert remains on your account for a minimum of 90 days. An extended alert remains on your credit report for seven years. With these alerts, you will receive free copies of your credit reports. Review these reports carefully, look for inquiries that you did not initiate, accounts you didn't open, and debts on your accounts that you can't explain. Check that your Social Security number, address, name, initials, and employers are correct. If you find fraudulent or incorrect information, get it removed. Keep checking your reports periodically to ensure that no new fraudulent activity has occurred.

The moral of the story is awareness of your personal information both in how you maintain your personal documents and in how it is shared with others.

- Make a list of at least 5 different ways that an identity thief may assume another's identity. Then beside each of these, list ways that you can protect that information.
- What are your views on who (consumers, government, businesses) should bear the burden of protecting consumers from identity theft? How should this be done?

What Can You Do to Protect Your Identity

With so many people becoming victims of identity theft and fraud each year, how can you make sure you do not become another part of the statistics? Being aware is the best weapon against identity theft.

The first step is to simply protect your credit, debit, and ATM cards as well as your account and PIN numbers. One way to do this is to only carry the cards that you plan to use. Keep the others in a safe place. Keep a list of all account



numbers and telephone numbers of the companies that issued your accounts. If your cards are lost or stolen, notify the companies quickly. If you notify the company before the cards are used, you have no liability. If your notification is received after the cards have been used, your liability is \$50 for each card. However, your liability for ATM or debit cards depends on how quickly you report the loss.

You should also monitor your accounts and bank statements each month. When ordering checks, pick them up from the bank instead of having them mailed to your home mailbox. Check your credit reports at least once a year to make sure that there are no mistakes or abnormalities. You can get one free credit report each year from each of the three credit bureaus (Equifax, Experian, and TransUnion) at <http://www.annualcreditreport.com> or by calling 1-877-322-8228. You need to check all three reports, not just one! Each bureau receives different information about you from different sources. You may want to check all three reports at the same time or spread your requests out over a twelve month period.

Another step you can take to protect your credit is to remove your Social Security Card or anything with your Social Security number from your wallet or purse. Only give your Social Security number when absolutely necessary. When you using the Internet, make sure you have current security software. Never give out your personal information on the Internet or the telephone unless you initiated the contact and you are sure who you are dealing with. Also, deposit your outgoing mail in post office collection boxes, or at your local post office rather than using an unsecured mailbox. Remove your mail from your mailbox as promptly as possible. Keep financial and personal papers in a secure place.

Even after an identity thief stops using a victim's information, victims struggle with the impact of identity theft. This can include increased insurance or credit card fees, inability to find a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime. This impact may continue for more than 10 years after the crime was first discovered. Thus it is crucial to invest the time and effort into protecting your identity and personal information.

Now that you have read some information regarding the prevention of identity theft, review the case study and answer the following questions:

- What are steps that Andrew should take to protect his personal information and identity from identity theft?
- What will you do to protect yourself from identity theft?

