Identity Theft

Family Economics and Financial Education

What is Identity Theft?

Identity theft occurs when someone wrongfully acquires and uses a consumer's personal identification, credit, or account information.

Identity theft can wreak havoc on an individual's credit report, cause a person to be arrested for crimes they did not commit, or open accounts using a person's name without the victim ever realizing their identity had been stolen.

Individuals whose identities have been stolen may spend countless weeks, months, or even years and hundreds of dollars resolving the problems identity thieves have caused.

The Federal Trade Commission (FTC) is an agency of the United States government that primarily focuses on consumer protection. The FTC helps pass laws that protect consumers against issues such as identity theft.

The number of identity theft complaints filed in 2008 was 313,982. – FTC

Identity theft complaints accounted for 26% of consumer fraud complaints in 2008, making it number one on the government's list of complaints. – FTC

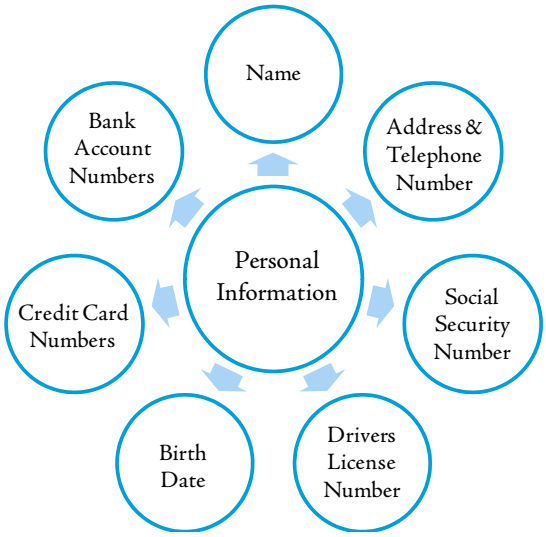
Approximately 7% of identity theft victims in 2008 were under 20 years of age. – United States Department of Commerce

10% of identity theft victims during 2005 reported personal expenses of more than $1200. – FTC

11% of victims in 2005 reported that it took 3 or more months to resolve the problems associated with identity theft. – FTC

Personal Information

Identity thieves try to obtain personal information from victims in order to steal their identities.



During a person's lifetime, there will be countless times when personal information is used during everyday transactions. These transactions are the activities upon which identity thieves thrive, because they require a person to share personal information, thereby increasing the possibility of someone stealing this information to commit identity fraud.

What Identity Thieves do with Information

Information identity thieves acquire can be used in numerous ways including:

- To apply for a new driver's license
- To open new bank and credit accounts
- To apply for credit cards or store credit accounts
- To obtain cash with bank cards
- To get a job
- To take out student loans
- To rent an apartment
- To make retail purchases
- To get a phone or other utilities
- To file bankruptcy
- To counterfeit checks
- To give a person's name during an arrest

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

How Do They Do It?

Stealing

Thieves can access personal information by stealing a purse/wallet, personal records from a workplace, tax information, bank or credit card statements, & pre-approved credit card offers from the mail.

Diverting Mail

Thieves can complete a change of address form and have the victim's bills and statements mailed to a different location.

Dumpster Diving

Information carelessly discarded into the trash can be stolen when a thief digs through the garbage.

Skimming

Thieves may steal credit or debit card information by attaching a device to card processors.

Phishing

Thieves use a form of electronic communication (usually email) to pretend to be a company or financial institution in order to get the victim to give up their personal information.

Pretexting

Thieves use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

Spyware

Software may be installed on the victim's computer, without their knowledge or consent, that monitors internet use, sends pop-up ads, re-directs the computer to other sites, and tracks key strokes.

Hacking

Thieves may break into a computer system and steal information.

Preventing Identity Theft

Key Guidelines

- Protect your Social Security number. Only give it out to trusted organizations and only when absolutely necessary.
- Keep usernames and passwords safe. Choose a combination of letters, numbers, and symbols not easily identified. Use different usernames and passwords for different sites and change them regularly .
- Select security check questions with answers only you would know (no mother's maiden name, school name, etc.).
- Check credit reports for errors <u>at least</u> once a year with all three reporting agencies. To stay constantly informed of credit report information, request a credit report from one of the three reporting agency every four months.
- Shred all documents that contain personal information or keep in a safe place .
- Don't give out personal information over the phone, through the mail, or on the Internet unless you've initiated the contact and are sure you know who you're dealing with.
- Be careful using the Internet. Only give out personal information when purchasing from a secure site.
- Protect your identity. Search your name occasionally to see if your name, picture, or other information is being used by someone else.

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

Although there is not an absolute way to avoid identity theft, there are actions that can be taken to minimize risk.

Information	Prevention
Wallets and Purses	• Do not leave in plain sight, and keep in a safe place at work and home. • Do not hang purses from a chair in a public place, and use purses that close securely. • Only carry what is necessary. Do not carry Social Security cards, passports, or birth certificates.
Credit, Debit and ATM Cards	• Close unwanted accounts in writing and by phone and cut up the card. • Memorize the PIN number and do not use easily accessible numbers such as a date of birth, anniversary, address, phone number, etc. Only carry cards that are used. • Sign back of credit and debit cards with signature and "Please See ID." • Do not give out account numbers unless making a transaction that is initiated by the consumer rather than responding to a telephone or e-mail solicitation. • Keep receipts and check statements regularly for any errors or signs of fraudulent use.
Credit Card Offers	• Shred credit card offers and applications. A cross-cut shredder is safest, because it will cut the document into crisscross pieces which are more difficult to reassemble. • Shred pre-approved credit cards that are not used. • The Fair Credit Reporting Act gives consumers the option to prevent credit reporting agencies from providing their credit file information to firms sending prescreened credit offers. Individuals can "opt-out" of receiving prescreened credit offers for 5 years by calling 1-888-567-8688 or at www.optoutprescreen.com
Mail	• Shred all credit card offers, bills, statements and anything else that contains personal information. Follow up if bills or statements do not arrive on time. • Deposit outgoing mail in post office collection boxes rather than unsecured mail boxes. • Contact the post office and request a vacation hold when unable to pick up mail. • Do not leave mail in an unsecured mailbox overnight or for a long period of time.
Email	• Keep your username and password protected. Use a password that is a combination of words, numbers, and symbols (Do not use names, birthdays, anniversaries, address, etc.). Do not write down usernames and passwords where they can easily be found. • Verify the source of any email asking for personal information by calling the company to confirm the email is from them and not a potential identity thief using their name. Also, check on the company with the Better Business Bureau.
Telephone	• Verify the source of any phone call asking for personal information by calling the company to confirm the phone call is from them and not a potential identity thief using their name. Use the phone number listed on your account statement or in the telephone book.
Computer Security	• Use anti-virus and anti-spyware software and update them regularly. • Do not click on links found in pop-up ads. Only download software from trusted websites. • Set web browser security to medium-high or high. Keep operating system and web browser software updated. • Do not give out any personal information unless making a purchase. • Watch for clues that might indicate a computer is infected with spyware. such as a stream of pop-up ads, unexpected toolbars or icons on the computer screen, keys that don't work, random error messages, and sluggish performance when opening programs or saving files. • If it is suspected that a computer is infected with spyware, immediately stop shopping, banking or doing any other online activity that involves user names, passwords, or other sensitive information. Then, confirm that the security software is active and current and run it to scan the computer for viruses and spyware, deleting anything the program identifies as a problem.

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

INFORMATION	PREVENTION
Social Networks, Blogs, & Chat rooms	• Consider joining only sites that limit access to posts to a defined group of users. Make sure you know how the site access works before joining. Don't join sites that allow anyone to view postings • Never post your full name, Social Security Number, bank or credit card information, address, or phone number • Avoiding posting information that could be used to identify you offline such as school, work, or other locations where you spend time • Use privacy settings to restrict who can access personal sites • Remember that once information is posted online, it cannot be taken back. Even if information is deleted, older versions may still exist on other people's computers and be circulated online • Only post information that you are comfortable with anyone viewing
Internet Purchases	• Look for "https" or a picture of a lock after the URL or in the bottom right hand corner indicating the site is secure • Do not give any personal information (name, address, credit card number, Social Security number, etc.) on a site if it is not secure (does not begin "https" or have a picture of a lock) • Enter the website address yourself rather than following a link from an email or Internet advertisement • Select passwords that do not contain easily available information such as birthdates, maiden name, children's names, etc. Do not write passwords down where they can easily be found • Use a credit card instead of a debit card when making online purchases
Social Security Number	• Memorize Social Security number • Keep Social Security card in a safe place (do not carry it in wallet) • Only give a Social Security number when absolutely necessary; when asked, inquire why it is needed, and how it will be protected; employers and depository institutions need Social Security numbers for taxes, other business may ask for a Social Security number to do a credit check or for record keeping
Credit Report	• Check credit reports with each of the three reporting agencies at least once a year. Consumers receive one free credit report from each of the credit reporting agencies every year, so ordering one credit report from one of the credit reporting agencies every four months will keep consumers up to date and constantly alerted to their credit report status • Immediately dispute any wrong information • Shred credit reports or store in a safe place where others cannot easily access them

3 CREDIT REPORTING AGENCIES

<u>Experian</u>
PO Box 2104
Allen, TX 75013-2104
Report Order:
1-888-397-3742
Fraud Hotline:
1-888-397-3745
www.experian.com

<u>Equifax</u>
PO Box 105873
Atlanta, GA 30348
Report Order:
1-800-685-1111
Fraud Hotline:
1-800-525-6285
www.equifax.com

<u>Trans Union</u>
PO Box 390
Springfield, PA 19064-0390
Report Order:
1-800-888-4213
Fraud Hotline:
1-800-6807289
www.tuc.com

TO ORDER A CREDIT REPORT FROM ANY OF THE THREE REPORTING AGENCIES, USE THE FOLLOWING WEBSITE: WWW.ANNUALCREDITREPORT.COM

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

RECOGNIZING IDENTITY THEFT

Early detection is key! The earlier an identity theft is discovered the quicker the fraudulent activity can be stopped.

Watch for the following signs:

- New accounts or charges that you did not make
- Calls from collection agencies
- Being denied credit when you do not believe there is reason to be
- Missing bills or mailed statements
- Incorrect information on your credit report

IDENTITY THEFT PROTECTION & INSURANCE

Many banks and other companies offer identity theft protection for a fee, usually between $5.00 and $35.00 a month, depending on the amount of services provided. These agencies closely monitor credit reports, credit scores, and personal information on the internet and alert the consumer whenever a change occurs in an effort to catch identity theft as early as possible. Most of the services provided can be completed by the individual at no cost. These services also assist in resolving any problems that identity theft may cause by contacting credit card companies, banks, and document issuing companies on behalf of the consumer.

Many organizations also offer identity theft insurance which limits the liability to the consumer if they are victims of identity theft by reimbursing them for some or all out of pocket expenses caused by the theft. When considering one of these services make sure to research exactly what they cover.

PERSONAL LIABILITY

Credit Cards

The Truth in Lending Act limits a person's liability for unauthorized credit card charges to $50.00 per card. To take advantage of this law, a person must write a letter within 60 days of the first bill containing the error. The dispute must be resolved within 90 days of the creditor receiving the letter. If an individual's card has been stolen, it should be reported and canceled immediately. If an individual's credit card number is used fraudulently, but the credit card itself is not used, the individual has no personal liability.

ATM & Debit Cards, Electronic Funds Transfers

The Electronic Funds Transfer Act provides protection. The amount a person is liable for depends upon how quickly he/she reports the loss. Cards reported within two business days of discovering the theft or loss are liable for a maximum of $50.00. Within 60 days, a person is liable for $500.00. After 60 days, a person may be liable for all of the money. A person should always call the financial institution then follow up in writing to report any losses. The consumer is not liable for any fraudulent charges made after a debit or ATM card has been reported stolen.

Checks

Stop payment and ask the financial institution to notify the check verification service. Most states hold the financial institution responsible for losses of a forged check if a person notifies the bank within a reasonable time.

WHAT TO DO IF IDENTITY

No matter how careful a person may be, identity theft can happen. If a person believes he or she may be a victim, they must follow these basic rules.

1. Act immediately to prevent any further damage and limit personal liability.
2. Keep a detailed record of all correspondence and phone records including the date, contact person, and any specific comments made or actions which will occur. Follow up all communication with letters sent via certified mail, return receipt requested, so you can document what was received and when.
3. Contact the three major credit bureaus and request a free "fraud alert" be added to the victim's credit report. Once a fraud alert has been added to a credit report, consumers are entitled to one free credit report from each of the reporting agencies. Once the credit reports are received, they should be reviewed very carefully and checked to ensure accuracy.
4. Close all accounts which have been opened fraudulently or tampered with, and file a dispute with the company. When opening new accounts, use different passwords and PIN numbers. Once the dispute has been settled with the company, ask for a letter explaining that the fraudulent debts have been discharged and the disputed account has been closed. This letter can help with resolving problems related to the account on the credit report.
5. File a police report with the local police or in the local community where the theft took place.
6. File a complaint with the Federal Trade Commission at http;://www.ftccomplaintassistant.gov

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona