Identity Theft

Southwest Research Center Federal Credit Union recognizes that identity theft can be a crime of enormous human and economic consequences. Identity theft victims suffer the frustration and stress of navigating a complex process to restore the damage caused by an identity thief.

Knowledge and awareness are key elements in the fight against this crime. We hope this information will provide insight into the fastest growing white-collar crime in America and help you avoid becoming the next identity theft victim.

What is Identity Theft?

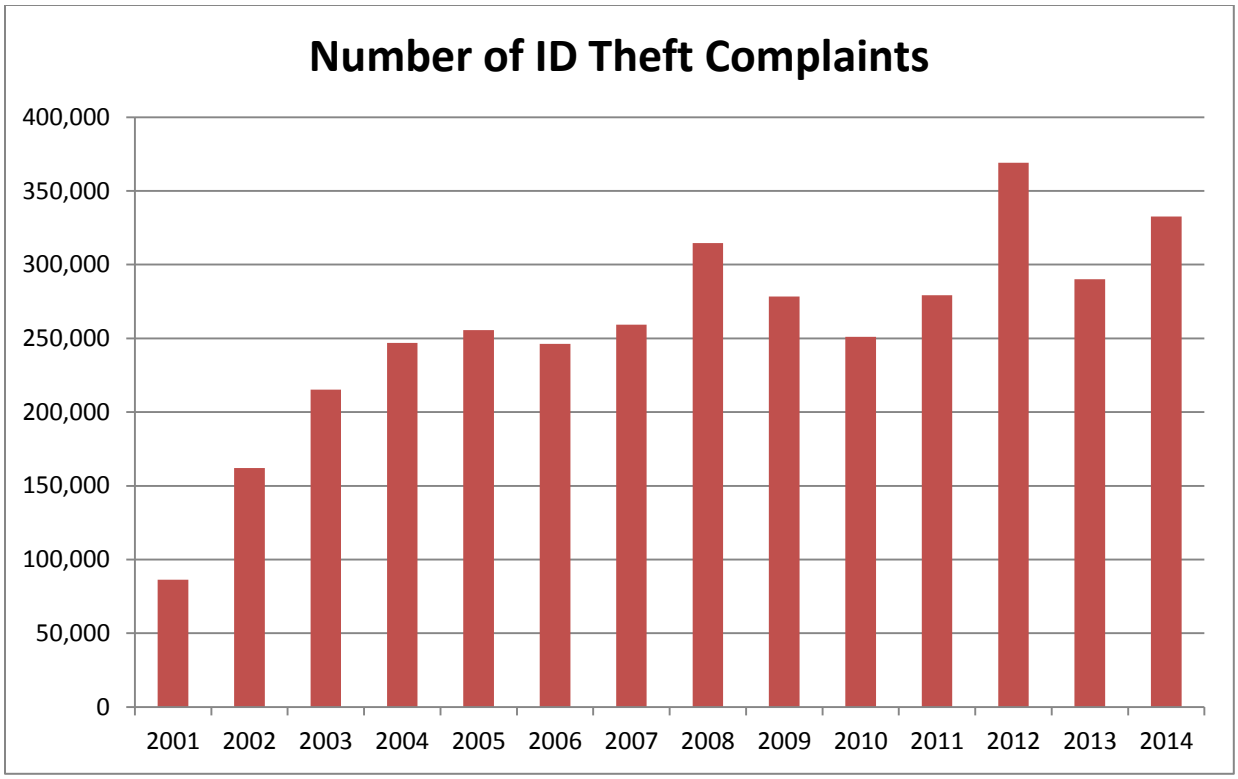
Short answer: Someone uses your identity to spend money and perform unlawful acts under your name and credit history.

Legal answer: Identity Theft occurs when someone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 to address the problem of identity theft. Specifically, the Act amended 18 U.S.C. § 1028 to make Identity Theft a federal crime and it's a felony with a 20-year maximum sentence. In July 2004, President Bush signed the **Identity Theft Penalty Enhancement Act** that guarantees a minimum of two years in prison for aggravated identity theft.

How Bad Is It?

The Federal Trade Commission (FTC) started collecting Identity Theft statistics in November, 1999. The latest FTC reports are available online. The reported numbers probably represent a small part of the problem. The FTC receives thousands of ID theft complaints each year.



The following data points were extracted from the FTC Consumer Sentinel Network Data Book for 2014

- Government documents\benefits fraud (39%) was the most common form of reported identity theft, followed by credit card fraud (17%), phone or utilities fraud (13%), and bank fraud (8%). Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (4%).
- Thirty-two percent of identity theft complainants reported they contacted law enforcement. Of those victims, 88% indicated a report was taken.
- Florida is the state with the highest per capita rate of reported identity theft complaints, followed by Washington and Oregon.

Tax or wage related fraud, represents 32.8% of the government documents/benefits fraud category. The IRS has a Taxpayer Guide to Identity Theft and they also have an Identity Protection Specialized Unit (1-800-908-4490) to assist when all other steps have been taken.

There have been several studies attempting to quantify the impact of identity theft. Annual statistics vary, but most agree with:

- approximately $50 billion loss to businesses and consumers
- 8 to 10 million American victims

What Can Happen?

Identity thieves have a buy now pay never shopping binge at your expense. California State Senator Debra Bowen notes that "Identity theft is one of the easiest, most risk-free crimes thieves can commit. They don't need a gun, a knife, or a getaway car. All they need is someone's Social Security number and a pen." ID thieves can use your name to:

- open credit card accounts
- open phone and utilities accounts
- get a bank loan or checking account
- file a tax return to get a refund
- buy a car
- get medical care
- and the most amazing part of all – **They can go to jail under your name**!

How Does It Happen?

Most victims don't know how their identity was stolen. Today's society of easy and legal access to information makes it easier than you may think. Data gathered through the Internet and electronic databases are potential sources for identity thieves, but low-tech means of stealing your information are more prevalent.

Dumpster Divers

An individual or business that fails to properly dispose of personal identification information, by shredding or mutilating, could find themselves susceptible to a "dumpster diver"--an individual who retrieves discarded material looking for anything of value.

Dumpster divers obtain account numbers, social security numbers, addresses, and dates of birth from financial, medical, and personal records--all of which they can use to assume an identity. The tax return season is like Christmas for identity thieves since so many people clean out their files.

You may follow a strict discipline of shredding sensitive documents, but what about the businesses that maintain your personal information. How do they dispose of records with your information?

Dumpster diving is a popular activity for thieves. An Internet search reveals several dumpster diver clubs you can join. You know you have reached a low point in life when you are a member of a dumpster diver club!

Mail Theft

Thieves check mailboxes looking for all kinds of interesting treasures.

- How many pre-approved credit card offers did you receive in the mail last week?
- Did you receive any statements containing your social security number, account numbers, etc.?
- Did you mail any bills with sensitive information?

Did you help your identity thief by **raising the red flag** on your mailbox to announce that your information is ready to be taken?

Your identity thief may take an easier route by simply submitting a change of address to temporarily divert your mail to a mailbox of a vacant house that he has access to. He only needs a week in most cases to receive a few pre-approved credit card offers. The post office will mail a change of address acknowledgement to both the new and old addresses. Contact your post office immediately if you receive a change of address notice unexpectedly.

Fake driver licenses and Social Security cards are for sale

Unethical businesses sell valid-looking drivers licenses and social security cards by publishing a ridiculous disclaimer that states the cards are novelty ID cards for novelty purposes only.

Insiders may sell your information

Your personal and sensitive information is maintained in records in several places. Your employer, dentist, doctor, county clerk and creditors just to name a few have information that is very valuable to an identity thief. A thief may be able to convince an employee to copy a few records for a few hundred dollars. Who's going to know?

Internet

There are web sites that sell your Social Security number. You can search for someone's birth date and even do a public records search. Use Google to search for your area code and phone number. You'll probably get a link to your name, address, zip code and a map to your house.

Google and other search engines provide a process to remove your phone number from their listings.

These links provide examples of information collection, opportunities to remove your name from some collections:

infospace	Their privacy policy states "you can review, correct, change or remove the personal registration information you provide to InfoSpace and that InfoSpace controls." It's not clear how to control your information. Try sending a request through their contact form
Network Advertising Initiative	Opt out of interest-based advertising at www.networkadvertising.org/choices/
Online Behavioral Advertising	Opt out of interest-based advertising at www.aboutads.info/choices/
MobileAppTracking	Opt out at www.optoutmobile.com/optout/index.html .
Do Not Track	Opt out at http://donottrack.us/
WhitePages.com	Their data police at www.whitepagescustomers.com/data-policy/ states "In order to stop further collection of information by us, you will need to stop using our products and services."
Yahoo!	You can opt out of interest-based ads at https://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html
SuperPages.com	Search for your listing at http://wp.superpages.com/ and then look for the "Remove Listing" link near the page bottom.
Zaba Search	In order for ZabaSearch to "opt out" your public information from being viewable on the ZabaSearch website, we need to verify your identity and require faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, cross out the photo and the driver's license number. We only need to see the name, address and date of birth. We will only use this information to process your opt out request. Please fax to 425-974-6194 and allow 4 to 6 weeks to process your request. - See more at: http://www.zabasearch.com/block_records/#sthash.rFF6mlkC.dpuf
Stop junk mail, email, & phone calls.	Stop junk mail, email, and phone calls with tips from http://www.obviously.com/junkmail/

Pretext Calling

Some thieves are very skilled at calling you or businesses to collect information about you. They call under the pretext of being someone else or you. They're looking for account numbers, your mother's maiden name, birth date, etc. Each call yields a little more information. Finally, they have enough info to convincingly assume your identity.

Please remember that the Southwest Research Center FCU will never solicit sensitive information through email or the telephone.

Credit Reports

Thieves obtain credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer or someone else who may have a legitimate need for and a legal right to the information. Your credit report provides all the information required to steal your identity -- social security number, birthday, phone number, account listing, employer, addresses, etc.

Scams

The Internet is full of scams and fraudulent efforts. Visit the Fraud Avengers website at http://fraudavengers.org/ to get informed.

Here are a few of the popular scams.

Lottery

You get an email claiming you just won a lottery. All you have to do is contact an agent to provide your sensitive information to claim the cash.

Nigerian E-mail

This scam is sent out to victims via letter, e-mail, and fax. It consists of a message stating the sender has a large sum of money and needs help transferring it out of Nigeria or some other place. As a reward for your help, the sender promises to pay you a few million dollars. Of course you only have to provide your bank account number, social security number, etc.

Visit http://home.rica.net/alphae/419coal/ to learn more about the Nigerian scams.

Online Auction Fraud

The fraud involves a fake ad on eBay to let someone "win" the bid and send in their money, but never send out the merchandise.

Phishing

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Phishers send an email or pop-up message that claims to be from a business or organization that you deal with - for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. What is the purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity.

By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

Visit the Anti-Phishing Working Group at http://www.antiphishing.org/ to learn more and to report phishing attacks.

Please remember that the Southwest Research Center FCU will never solicit sensitive information through email or the telephone.

Visit http://www.fraudwatchinternational.com/phishing-alerts for a list of the latest phishing attempts.

You've Won A Prize

The thieves call you with the exciting news of a prize you just won. All they need is a credit card number, social security number, etc, to validate the award.

Preventive Measures

You can never be 100% protected from identity thieves, but you can do a lot to make it difficult for thieves to get your information. Early detection is the key. An average of 12 months passes by before most people realize they are victims of Identity Theft.

Free Annual Credit reports

Credit bureaus, also known as Credit Reporting Agencies, maintain your credit history files. Order your credit report at least once each year from all three of the major credit bureaus to detect evidence of identity theft. Reviewing your credit report is the best tool to detect identity theft.

Thanks to the Fair and Accurate Credit Transactions Act (FACTA), all Americans can receive one free credit report from each bureau annually. Identity theft victims can receive two copies from each bureau in the year the theft occurs. The free annual credit reports can be ordered online, by phone, or by mail. Free credit reports requested online are viewable immediately.

Online:www.annualcreditreport.com

Phone: 1-877-322-8228

Mail: Mail the request form to:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

You can order all three free credit reports at the same time, but it's a better idea to order a credit report from a different credit bureau at four month intervals to increase your odds of detecting identity theft activity throughout the year. Your spouse should order their credit reports two months after you do. This will provide a snapshot of your credit several times throughout the year.

Here is a sample schedule. Setup the reminders on your phone right now.

January **YOU** ***Equifax***	February	March **SPOUSE** ***Equifax***	April
May **YOU** ***Experian***	June	July **SPOUSE** ***Experian***	August
September **YOU** ***TransUnion***	October	November **SPOUSE** ***TransUnion***	December

Review your credit reports thoroughly for suspicious charges and credit inquires that represent attempts to open an account in your name. Incorrect addresses are also a clue a thief may have attempted to get a credit card in your name.

Additional Credit reports

The three major credit bureaus are Equifax, Experian, and TransUnion. Each bureau will sell you credit reports for a small fee if you want additional credit reports after ordering your free reports. You can order additional credit reports through a credit bureau web site, by phone, or by mail as shown below.

You can request additional free credit reports when you submit fraud alerts.

Credit Bureau Contact Info

Equifax	**Order Credit Reports** Online: www.equifax.com Phone: 1-800-685-1111 Mail: P.O. Box 740241, Atlanta, GA 30374-0241 **Report Fraud** Phone: 1-800-525-6285 Mail: P.O. Box 740241, Atlanta, GA 30374-0241
Experian	**Order Credit Reports** Online: www.experian.com Phone: 1-888-EXPERIAN (397-3742) Mail: P.O. Box 2104, Allen TX 75013 **Report Fraud** Phone: 1-888-EXPERIAN (397-3742 P.O. Box 9532, Allen TX 75013
TransUnion	**Order Credit Reports** Online: www.transunion.com Phone: 1-800-916-8800 Mail: P.O. Box 1000, Chester, PA 19022

	Report Fraud Phone: 1-800-680-7289 Mail: Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Free Specialty Reports

The FACT act has made other specialty reports available free of charge.

Increase Your Awareness

These situations should raise your suspicions:

Credit Report Entries

- Accounts you didn't open
- Debts you can't explain
- Inquiries from companies you haven't contacted
- Unknown addresses

Other Indicators

- Your mail is interrupted
- You receive an unexpected change of address notification
- Bill collectors are calling you about unknown debts
- Your credit score takes an unexpected decline
- You start receiving statements from companies you have no relationship with
- Credit cards arrive in your mailbox that you didn't apply for

Stop those pre-approved credit card offers

Are you getting tired of all those pre-approved credit card offers in your mailbox? You can stop them today.

Creditors pre-screen your credit history with the one or more of the credit bureaus before they mail a pre-approved credit card offer to you. That's where you have the power. You can stop the credit bureau pre-screening by calling 1-888-5OPTOUT (1-888-567- 8688).

The major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers. Make the call for each person in your family. You can also opt out through a single web site at https://www.optoutprescreen.com .

Passwords

Put passwords on your credit card, credit union, retirement, and phone accounts and with any other financial relationship you have. This is a password or pass-phrase that you should be asked for each time you call or visit your financial institution. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Test the businesses occasionally to ensure they continue to ask for your password.

You definitely want to avoid the situation where the identity thief sets up a password of his choosing with your financial institutions. Imagine the surprise when you call your credit card company and they inform you that they can't share information with you without the password! It has happened. Put passwords on your accounts before the thief has an opportunity to do it.

Guard your mail from theft

Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from an unlocked mailbox. Replace curbside mailboxes with lockable boxes. Your postman won't be able to pick up mail from your box but he'll still be able to deliver it.

Contact the post office to request your mail be held at the post office if you will be away for a while. You can request a mail hold online at https://holdmail.usps.com/holdmail.

Pick up check orders from your credit union instead of having them mailed to your house.

Be aware of when monthly bills, statements, and other sensitive information normally arrive in your mailbox. Missing mail could be an indicator that identity thieves are stealing your mail. A missing credit card bill could mean your thief has taken over your credit card account and changed your billing address. Contact the credit card issuer if you apply for a credit card and it doesn't arrive in the mail within a reasonable amount of time.

Protection against insiders

Contact your employer and businesses that maintain records on you. Find out who has access to your personal information and how it is handled. Verify that they keep your records in a secure location. Read their privacy policy.

Does your dentist leave patient records unlocked after business hours giving full access to the cleaning crew? Ask your dentist why he/she feels comfortable putting you at risk. Don't accept the answer "*my cleaning crew is bonded*". Thieves are not concerned about that. A bonded crew may protect your dentist but it won't protect you.

Protect Your Computer

Visit StaySafteOnline.org to learn about potential threats and ways to protect your computer.

Here are practices to consider.

- Know who you're dealing with online.
- Be sure to set up your operating system and Web browser software properly and update regularly.
- Back up important files.
- Protect your children online.
- Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.
- Use strong passwords or strong authentication technology to help protect your personal information.
- Learn what to do if something goes wrong.

Signs of a malware infection may include:

- Slow computer
- Automatic reboots while running other programs
- More spam messages
- More popup advertisements even when not using the Internet

Use Public Computers with Caution

Public computers are convenient. You find them at libraries, coffee shops and universities to name just a few places. The convenience is nice but these computers are a potential source of data for your identity thief. You don't know who's looking over your shoulder or who uses the computer before or after you.

Don't enter sensitive information. A public computer is not a place to enter data like your credit card and social security numbers.

Here are a few ideas to consider:

- Try to keep the screen and keyboard hidden from the view of others. Thieves use binoculars to observe data from a distance so be conscious of viewing areas above and behind you. This applies to ATM use as well.
- Always log off of web sites when you're finished instead of just closing the browser window.
- Never accept the option to save your user name and password.
- Erase temporary files, history, and cookies before leaving.
- Disable the AutoComplete feature.

Despite your best efforts, you are still vulnerable to spy ware and key-logger software installed on the computer before you arrived. This software collects your keystrokes and can email them to the thief. Some of these programs are foiled by copy and paste techniques. For example to enter your password, open a large text file. Copy and paste each letter of your password from the text file and paste it in the browser window.

It makes more sense to completely avoid entering sensitive data in a public computer. Use it for web surfing and reading the news.

Protect Your Social Security Number

The Social Security Act was enacted in August 1935. A byproduct of this legislation was the decision to assign every citizen who qualified for social security benefits and/or contributed a social security tax the unique record identifier that is widely known as the Social Security Number. The intention from the beginning was that the SSN be a primary identifier only within the Social Security Administration. What happened?

Your social security number is used everywhere today. It's the perfect unique identifier used by computer databases in all aspects of business. Sadly, the SSN has even been used as a student ID in universities. The ubiquitous use of the SSN is exactly what makes it so valuable to the identity thief.

- Give your SSN only when absolutely necessary. Sometimes businesses want your SSN for simple record keeping. Ask to use other types of identifiers when possible.
- Don't put your SSN on your checks and don't let a merchant do it either.
- Don't carry your social security card; leave it in a secure place.
- Ask businesses not to print your SSN on documents sent through the mail.
- Don't list sensitive information on social networking sites like Twitter, Facebook, or LinkedIn.
- If a business/organization forces you to provide your SSN, ask about their data protection policies and how they handle data breaches.

Destroy Your Hard Drive – Computer & Copy Machine

Don't throw away your computer without completely destroying the data on the hard drive.

Digital copy machines contain hard drives too. Has your copy machine ever been used to copy, scan, or print documents with sensitive information? Read "Copier Data Security: A Guide for Business" from the Federal Trade Commission about copier data security.

What's in your wallet or purse?

Minimize the identification information and the number of credit cards you carry to what you'll actually need. What will your identity thief get if he stole your wallet or purse right now? Take some time now to make copies of the important items - credit cards, ID cards, ATM cards, etc. Make a contact list of the fraud departments for each account.

Do you really need to carry two or more credit cards?

You rarely need your social security card - please don't carry it with you.

Monitor and Protect Financial Accounts

Check your statements thoroughly and frequently. Online accounts make this job much easier and increase your odds of early detection.

Consider the following if you have to use checks:

- Check printing ideas
    - Use initials for your first and middle name. The thief may have to guess at your name when forging your check.
    - Use your cell phone instead of your home number.
    - Never print your social security number or driver license number.
    - Use a P.O. Box address if you have one instead of your home address.
- When writing a check to pay a credit card account, only list the last 4 digits on the For line.

Protect Your Paper Documents

You have documents everywhere -- in your car, your home, your desk drawer at work. Lock up any documents containing identifying information. Don't make it easy for others to have access in open view or in an unlocked container.

Shred, Shred, Shred

Identity thieves love your garbage because it's a potential treasure of identification information about you. Put your garbage on the curb on the day of collection. Don't allow a thief to have access to your garbage during the cover of darkness.

Get in the habit of using a **cross-cut (**not a strip type**)** shredder to shred all documents with information you're not willing to share with your thief. Inquire about the shredding policies of businesses that maintain information about you.

Check out the Southwest Research Center Federal Credit Union web site for announcements about Free Shred Days.

You are a victim. What do you do?

Most victims experience a wide range of emotions when they discover someone has been using their name to commit fraud. It's a very frustrating time but there is a lot you can do. Don't give up. Get organized and fight back.

Read the information presented her and this resource from the FTC, Immediate Steps to Repair Identity Theft . You can also call the ID Theft Resource Center at (888) 400-5530 or email them at Victims@idtheftcenter.org.

Take Good Notes

Grab a pad of paper and a pen. You need to take accurate and thorough notes as events and conversations occur. There will be a lot of activity initially. Transfer your notes to a word processor document if you have a computer. A table with the following categories works well. Ideally, you'll be able to sort the table by company name, date, etc. A sorted table can be very handy when you are doing follow-up actions. You may end up in court someday. Good notes will be valuable.

Example

Date yyyy mm dd	Time	Company/Agency	Point of contact - name and phone	Comments
2015 09 28	10:00 am	Police Department	Officer John Doe (110) 123-7654	Filed police report. Gave officer my completed ID Theft Victim's Complaint & Affidavit form. Asked officer to submit an NCIC Identity Theft File report.
2015 09 31	1:23 pm	Acme	Bill Smith, manager, (110)555-1212	Will accept standard affidavit. He said he'll submit a correction to my credit bureau account.
2015 10 02	8:00 am	Acme	(112) 123-4567	Mailed affidavit to Bill Smith. Certified mail receipt number 123678.

2015 10 05	8:32 am	Some Credit Card Company	George Johanson, fraud department supervisor. (110)123-4576	George said he'll mail copies of the fraudulent applications to me after my written request arrives at his office. He closed the fraudulent account.
2015 10 13	11:00 am	Acme	Bill Smith (110) 555-1212	Talked to Bill Smith. Verified that he received my affidavit mailed on Sep 9, 2013.

- Date -use a format like yyyy mm dd to improve sorting
- Company/Agency - be consistent with names to improve sorting.

You will accumulate a multitude of documents very quickly. It helps to organize them in a 3-ring binder as soon as possible.

Keep track of how much money you spend while fighting your identity thief. In September 2008, President Bush signed the Identity Theft Enforcement and Restitution Act of 2008. This law requires that in cases where convicted ID thieves are ordered to pay restitution, the convicted thief will pay the victim an amount "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."

Download a Guide from the FTC

Download this Federal Trade Commission guidebook for assisting ID theft victims. Look for the section titled “Checklist for General Steps Addressing Identity Theft".

Order your credit reports

Order your credit reports online to have immediate access to your thief's activity.

- www.experian.com
- www.equifax.com
- www.transunion.com

It's worth spending the few dollars (if required) to get immediate access to at least one of your credit reports so that you can start fighting back today. **You can get an immediate online version of your credit reports for free** if you haven't taken advantage of your free annual reports through www.annualcreditreport.com.

You're also entitled to a free credit report from each credit bureau when you submit a fraud alert. Contact the credit bureaus if you don't receive a letter from them within 10 days

following your fraud alert submission. The letter will explain the method to obtain a free credit report from them.

Ideally you want to submit the fraud alert first. Consider getting your online credit report first because a fraud alert may prevent you from gaining access to your credit report online. Submit a fraud alert as soon as possible.

Submit fraud alert

Fraud alerts can help prevent an identity thief from opening additional accounts in your name. The Fair and Accurate Transaction Act (FACTA) added a new section to the Fair Credit Reporting Act (FCRA) that provides for three varieties of alerts that consumers may add to their files with nationwide consumer reporting agencies -

- Fraud Alert
- Extended Fraud Alert
- Active Duty Fraud Alert

The alerts differ in their initiation requirements, time periods, and limits on creditors. All three varieties of alerts must state that the consumer does not authorize new credit (other than an extension under an existing open-end credit account, that is, a credit card), an additional card on an existing account, or any increase in the credit limit of any existing account.

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Verify information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See the Federal Trade Commission's guidance on Correcting Fraudulent Information in Credit Reports to learn how. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

- **Fraud alert** -
  - Creditors must utilize "reasonable policies and procedures" to form a reasonable belief that the creditor knows the identity of the person making a credit request.
  - Alert stays active for **90 days**.
  - Consumer can request one free credit report from each bureau.
  - **A fraud alert at any of the credit bureaus automatically initiates an alert at the other two.**
    - You can also submit alert online.
    - Call any of the following numbers 24 hours a day:
      - Equifax 1-800-525-6285

        - Experian 1-888-397-3742
        - TransUnion 1-800-680-7289
- **Extended fraud alert** -
    - Consumers may provide a telephone number in the alert which the creditor must use to verify the requester's identity unless the consumer designated another reasonable method of contact.
    - Alert stays active for **7 years**.
    - Consumer must submit an identity theft report which includes a report from a law enforcement agency. Consumer is subject to criminal penalties for submitting false reports.
    - Consumer is removed from marketing lists for 5 years, which the bureaus sell to lenders and insurance companies for use in solicitations.
    - Consumer can request two free credit reports from each bureau within 12 months of submitted extended fraud alert.
- **Active duty alert -**
    - Consumers on active military duty can add an alert of their status to their files. Consumers on active duty include reservists who are on active duty, other than at their usual station. Once a military consumer requests the active duty alert, it will become part of his/her credit report for a **12 month period**.
    - Consumer is removed from marketing lists for 2 years, which the bureaus sell to lenders and insurance companies for use in solicitations.
    - Does not entitle consumer to free credit report.
    - Creditors must utilize "reasonable policies and procedures" to form a reasonable belief that the creditor knows the identity of the person making a credit request.

Contact the Federal Trade Commission and the ITRC

The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission helps victims of identity theft by providing them with information to help resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for action.

Before calling the police, complete an ID Theft Victim's Complaint & Affidavit form which organizes information that will be helpful to you and the police. You can print the completed form to give to police. You can also contact the FTC by:

- Telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502. This number is answered by a representative that will provide advice and immediate actions you can take.
- Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington DC 20580
- Online: http://www.consumer.ftc.gov/features/feature-0014-identity-theft

You can also contact the **Identity Theft Resource Center** (ITRC) to ask for assistance. Send the ITRC an email at Victims@idtheftcenter.org or call the ITRC Victim Assistance Center Toll Free (888) 400-5530.

Make a police report

Try to make a report with the local police and the police department(s) with jurisdiction where your identity thief is using your name. Some identity theft victims have reported resistance in the past from the police department to file a report. Be persistent.

Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report. Ask to file a "Miscellaneous Incidents" report if the police are reluctant to take your report. You can also try another jurisdiction, like your state police.

Ask the police to submit an Identity Theft File to the FBI's National Crime Information Center (NCIC). This provides a means for all law enforcement officers around the country to discover a potential identity thief when they run a query into the NCIC system. This can happen when the police pull over your thief for a normal traffic stop.

The combination of an ID Theft Affidavit and your police report make an **Identity Theft Report** which can be used to:

- Get fraudulent information removed from your credit report
- Stop a company from collecting debts that result from identity theft, or from selling the debt to another company for collection
- Place an Extended Fraud Alert on your credit report
- Get information from companies about accounts the ID thief opened or misused

Even if the police can't catch the identity thief in your case, having an Identity Theft Report can help you when dealing with creditors.

Contact your financial interests

Report the identity theft to your credit union, credit card issuers, and any other activity that you have a financial relationship with. Add a password to your account if you haven't done so previously (don't use your mother's maiden name). Close the accounts that you know or believe have been tampered with or opened fraudulently.

Many of these institutions have a full time staff to work with fraud cases. Some fraud departments operate in the late evening hours so don't wait until the next day to start your fraud reporting. Search the company web sites for access to the fraud department telephone numbers.

Most financial institutions will want you to complete an affidavit that provides information about the fraudulent activity. The Federal Trade Commission provides a standard affidavit form that may be acceptable to most of the institutions.

Some fraud departments represent several different businesses. Ask them to search all of their databases for fraudulent activity using your social security number.

It's important to follow up in writing. Mail all correspondence to the fraud departments with certified, return-receipt mail. Pick up several blank forms from the post office to save time on future mailings. You can check the delivery status of certified mail online.

The fraud departments may ask for notarized documents. Ask them to waiver this requirement. The costs start to add up.

Contact each merchant your thief did business with

The credit reports show where your thief has been spending your money and contact info for each merchant. Call each merchant to inform them of the theft and request copies of credit applications, charge slips, etc. implemented by your thief. Ask them to submit corrections to the credit bureaus to remove entries from your credit report. Take good notes of your conversation and follow-up your conversation with a letter sent by certified, return-receipt mail.

Section 609e "Information Available to Victims" of the Fair Credit Reporting Act (FCRA) requires businesses to provide this information ***if the victim makes the request in writing***. Companies must provide the records at no charge to you within 30 days of receipt of your request and supporting documentation. The company may ask for proof of your identity, a copy of the police report and a completed affidavit.

You may prevent businesses from reporting information about you to consumer reporting agencies if you believe the information is a result of identity theft. You must send your request to the address specified by the business that reports the information to the consumer reporting agency. The business will expect you to identify what information you do not want reported and to provide an identity theft report.

File disputes with credit bureaus

The credit bureaus and the organization that provided the information to the bureau have a responsibility to correct errors and entries caused by your identity thief. File a dispute with each bureau that is reporting incorrect information and the company that submitted the information. TransUnion, Experian, and Equifax all have dispute information online.

Identity theft is not the only cause for credit report errors. A 2004 study found that one in four credit reports contains errors serious enough to cause consumers to be denied credit, a loan, an apartment or home loan or even a job.

Contact check verification companies

Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief. Inform the verification companies that you are an identity theft victim. Keep notes and follow up with a letter.

Submit a ChexSystems® identity theft security alert by visiting this link or calling 888 478-6536. ChexSystems® customers will be notified of the security alert each time they inquire about you. The security alert may prevent your identity thief from opening a bank account in your name. You can submit a 90-day or 5-year alert. You will have to complete an affidavit form.

Make sure ***your credit union or bank*** submits a report to the ChexSystems® Lost or Stolen Check Hotline which alerts retailers and other financial institutions to the missing checks or information. Insist that your credit union or bank contact ChexSystems® if they're not aware of the hotline.

- CheckRite - 1-800-766-2748
- ChexSystems® - 1-800-428-9623 (closed checking accounts)
- CheckCenter/CrossCheck - 1-800-843-0760
- Certigy/Equifax - 1-800-437-5120
- National Processing Company (NPC) - 1-800-526-5380
- SCAN - 1-800-262-7771
- TeleCheck - 1-800-710-9898

Contact utility and service provider companies

Contact utility and service provider companies such as: the local telephone company; long distance telephone company; cable company; internet service provider; and electric, power, gas or water providers. Alert each company or service provider of the theft of your identity and inform them that attempts may be made to open new service using your identification information. Request that any new request for service be confirmed with you and provide a telephone number and mailing address. Keep a copy of all of these requests.

Debt Collectors

Collection agencies may contact you about debts created by your thief. If you ask, a debt collector must provide you with certain information about the debts you believe were incurred in your name by an identity thief - like the name of the creditor and amount of the debt.

The Collection Agencies and Identity Theft fact sheet at the ID Theft Resource Center is a good source of information on this topic.

IRS Problems

The IRS publication "Identity Theft Prevention and Victim Assistance" is available at http://www.irs.gov/pub/irs-pdf/p4535.pdf.

Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information which includes any type of electronic communication, such as as text messages and social media channels.

Fraudulent tax return-related identity theft increased nearly six percentage points from 2006 through 2008. The IRS opened the Identity Protection Specialized Unit on October 1, 2008. This unit will help resolve identity theft victims' issues when previous contacts with the IRS have not resolved a fraudulent tax issue**. Victims can call a dedicated toll-free number, 800-908-4490**, Monday - Friday, 8:00 a.m. - 8:00 p.m. your local time (Alaska and Hawaii follow Pacific Time). They will want a police report or a completed IRS Identity Theft Affidavit, Form 14039

The unit will reduce taxpayer burden by providing individualized assistance, including:

- A single customer service representative to work with each identity theft victim to answer questions and resolve his or her issues.
- A simplified process to verify taxpayer identity and identity theft.
- A place for taxpayers to self-report identity theft before it impacts their tax accounts
- A place for taxpayers to self-report incidents where they may be at risk for identity theft because their personally identifiable information has been compromised (for example, stolen purse/wallet).
- In addition, the unit will assist taxpayers who have already had their tax accounts impacted by identity theft but have not yet had their issues resolved. The unit will refer taxpayers to the IRS area that is working the identity theft issue and also collaborate with that area to monitor the case through resolution.

If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity, credit report, or other activity, you need to provide the IRS with proof of your identity.

You should submit a copy, not the original documents, of your valid Federal or State issued identification, such as a social security card, driver's license, or passport, etc, along with a copy

of a police report or Federal Trade Commission Identity Theft Affidavit. If the FTC Affidavit (, Form 14039) is not notarized, a witness (non-relative) must sign it.

Please send these documents using one of the following options:

Mailing address:
Internal Revenue Service
P.O. Box 9039
Andover, MA 01810-0939

FAX: Note that this is not a toll-free fax number 1-978-247-9965

Mail Theft

Submit a complaint to the U.S. Post Office if you suspect your identity thief used your mail.

Credit Freeze

A credit freeze, also known as a security freeze, provides a method to prevent anyone from looking at your credit report without your involvement. You have to provide a personal identification number (PIN) to the credit bureau to "thaw" out your credit report and allow access by someone you authorize. This will stop your thief from applying for new credit where a merchant requires a credit report to authorize credit.

You have to contact each credit bureau where you want to implement a credit freeze. How much does it cost? The laws controlling the cost to freeze and thaw your credit account vary from state to state. It's free for identity theft victims in most states. Get your police report to prove that you are an ID theft victim and you may get this protection for free. Visit this Consumer's Union site to read about laws for your state.

Stolen Passport

You can report a stolen or lost passport by phone or submitting a DS-64 form through the mail.

Phone	Call 1-877-487-2778. Operators are available 8 A.M. to 10 P.M. ET Monday-Friday, excluding federal holidays
Mail	Complete, sign and submit Form DS-64: Statement Regarding a Lost or StolenPassport to: **U.S. Department of State** **Passport Services** **Consular Lost/Stolen Passport Section** **1111 19th Street, NW, Suite 500** **Washington, DC 20036**

Stolen Driver License

Report your stolen license to the police. Bring your police report to your local driver license bureau and try to convince them to declare the stolen license as fraudulent and issue you a new driver license number. You may encounter resistance. The driver license bureau may want proof that your license was used in a crime.

Getting the stolen license identified as fraudulent may prevent the thief from opening a financial account in your name and may lead to an arrest if he presents your license to a police officer during a traffic stop or other situation.

Stolen Birth Certificate

Make a police report to have proof you reported the theft.

Report a stolen or lost birth certificate to the agency that maintains the record of your birth such as the Bureau of Vital Statistics that serves the town where you were born. Some states will flag your record to require a picture ID for future issuance of records in an effort to protect you from identity theft.

Stolen Social Security Card

Social Security does not take reports of a lost or stolen Social Security cards or numbers. If you have lost your card, you may apply for a replacement but Social Security takes no action just because it has been lost or stolen.

Follow up

Keep excellent records and follow up on actions to ensure problems are resolved. Getting fraudulent entries cleared from your credit reports can be a slow and frustrating process. Be patient, but persistent. The Fair Credit Reporting Act provides regulations on the process of correcting credit report errors.

Mobile Security

Most everyone you know has some type of mobile device. Smart phones, tablets, and iPads are everywhere and so is the sensitive data that is stored or transmitted by these devices.

We need to maintain the same level of security on mobile devices as we do with other forms of communication and information management.

I Know Where You Are

Geotagging

Most smart phones have the ability to "geotag" pictures taken with the phone. The exact latitude and longitude can be embedded in the picture itself. Geotagging can be a great feature if you want to remember the exact location where you took a picture. Unfortunately, criminals can use geotagging information and other public information to "cybercase" you.

Let's say you are posting a picture of an expensive television on Craig's list. You may not display your home address, but the geotagging you left in the picture will identify the exact location. Your ad may also state to call after 5PM which could indicate you're not home until after that time. This is helpful information for your burglar.

Search on the Internet for "How to disable geotagging" for your phone and other mobile devices you take pictures with. Only turn geotagging on when you want to capture the exact location of the picture.

Geotagging and other data is part of the "Exchangeable Image File Format" known as Exif data. Search for Exif software to view, manage, and remove Exif data from your photos you post on public sites. You can find Exif tools in the Apple iTunes and Google Play Store as well as browser add-ons.

I'm on Vacation

It's fun to share your travel photos on Facebook and other social media sites. It's also valuable information for burglars. Consider waiting until your return to post about the vacation you just finished.

Don't Share Personal Information (like your birthdate) Online

Identity thieves must love that many of their victims provide helpful identifying information on public social media sites like Facebook.

Social media sites most likely collect personal information for targeted marketing and for sale to 3rd party marketers. Ignore requests for personal information when you can. Is it really necessary to display your exact birthday on Facebook? Your real friends and family will know your birthday.

What if your phone was lost or stolen?

It's possible to lose or misplace your phone or have it stolen. Increase the difficulty for an identity thief that gets your phone with a strong password.

Some phones will let you use your fingerprint or to draw a pattern on the screen to unlock the phone.

Some phones will let you determine a message that is displayed on a locked screen. Enter a message asking them to call your spouse or friends telephone if the phone is found.

Public Networks

Public Wi-Fi networks can be handy but you must remember these are not secure environments. This is not a time to enter a user name and password on any online account.

Turn off Bluetooth or Wi-Fi when you don't need it to avoid unintended connections to networks.

Software

- Keep your mobile operating system updated with the latest version.
- Install mobile security software. Some phones have security software installed by default or have free versions available for download. They may provide features to remote wipe phone date, locate your phone, and even take a picture of your thief.
- Check the app reviews and ratings before downloading. Do an Internet search to look for comments about the app you're thinking of downloading. Don't download apps from unknown sources.

Prepare Your Phone for Discarding

You need to remove all personal information from your phone before you get rid of it.

- Backup your personal data
- Remove the SIM card is possible.
- Search Internet for guidance on the Factory Data Reset for your phone.