

I D Theft

Southland 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 crime in America and help you avoid becoming an 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. It's a felony with a 15-year maximum sentence. In July 2004, President Bush signed the [Identity Theft Penalty Enhancement Act](#) that guarantees a minimum of two years in prison.

How Bad Is It?

The Federal Trade Commission (FTC) started collecting Identity Theft [statistics](#) in November, 1999. The numbers probably represent a small part of the problem, but it is clear that ID theft is on the rise. The FTC receives an increasing number of ID theft complaints each year:

Year	# of complaints
2000	31,117
2001	86,212
2002	161,896
2003	215,177
2004	246,847
2005	255,565

In 2005, credit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%).

The percentage of complaints about "Electronic Fund Transfer" related identity theft more than doubled between 2002 and 2004 and was the most frequently reported type of identity theft bank fraud in 2005. The major metropolitan areas with the highest per capita rates of reported identity theft are Phoenix-Mesa-Scottsdale, AZ; Las Vegas-Paradise, NV; and Riverside-San Bernardino-Ontario, CA.

Identity Theft Victims By State - 2005			
Rank	Victim State	Victims per 100,000 population	Number of Victims
1	Arizona	156.9	9,320
2	Nevada	130.2	3,144
3	California	125.0	45,175
4	Texas	116.5	26,624
5	Colorado	97.2	4,535

The FTC sponsored a [study](#) in 2003 that revealed these troubling annual statistics.

- \$47 billion loss to businesses
- \$5 billion to consumers
- 9.91 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 – the most frequent abuse
- open phone and utilities accounts
- get a bank loan or checking account
- file a tax return to get a refund
- buy a car
- 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 the 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 acknowledgment to both the new and old addresses. Contact your post office immediately if you receive this notice unexpectedly.

Fake drivers 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. One web site charges \$79 for a drivers license and \$99 for a Social Security card -- steep prices for "novelty" items.

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. Visit [Google](#) and 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 provides a [web site](#) to remove your phone number from their search engine.

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 Southland Federal Credit Union 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 [Fraud Watch International](#) to view a list of currently used scams. Here are a few of the popular scams.

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.

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. Read about recent phishing attacks at www.antiphishing.org/

Please remember that the Southland Federal Credit Union will never solicit sensitive information through email or the telephone.

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 pass 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.

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.

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

Other Indicators

- Your mail is interrupted
- 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](#).

Passwords

Put passwords on your credit card, credit union, retirement, and phone accounts and with any other financial relationship you have. 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.

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

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.

Protect Your Computer

Learn about potential threats and ways to protect your computer. Here are the top 8 cyber security practices recommended by the [National Cyber Security Alliance](#).

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

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.
- 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.
 - With Microsoft Internet Explorer, click Tools then Internet Options. On the General tab, click Delete Files, Delete Cookies and Clear History buttons.
- Disable the AutoComplete feature.
 - With Microsoft Internet Explorer, click Tools then Internet Options. On Content tab, click AutoComplete and uncheck the four boxes.

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 is even used as a student ID in many 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.

What's in your wallet or purse?

Minimize the identification information and the number of cards you carry to what you'll actually need. What will your identity thief get if he stole your wallet or purse right now? Do you really need to carry two or more credit cards? 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.

Shred, Shred, Shred

Get in the habit of using a cross-cut shredder to shred all documents with information you're not willing to share with others. Inquire about the shredding policies of businesses that maintain 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.

You are a victim. Now what do you do?

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 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.

- Date –use a format like 2006 07 21 to improve sorting
- Time
- Company/Agency – be consistent with names to improve sorting.
- Point of contact name and telephone number
- Comments

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

Order your credit reports

Order your credit reports online to have *immediate* access to your thief's activity. You'll get free credit reports through the mail when you submit a fraud alert, but you should consider ordering at least one credit report online.

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 online version for free if you haven't taken advantage of your free annual reports through

www.annualcreditreport.com.

You can get your online reports for a small fee if you've already used your free annual reports.

- www.experian.com
- www.equifax.com
- www.transunion.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 your credit report within 10 days following your fraud alert submission.

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) adds 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 and 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.

- 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. 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.

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 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.

Get a copy of the police report in case the credit card company or others need proof of the crime. You'll need a police report if you decide to submit an Extended Fraud Alert. Even if the police can't catch the identity thief in your case, having a copy of the police report(s) 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).

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.

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.

The fraud departments may ask for notarized documents. Ask them to waive 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. A provision of the new Fair and Accurate Transactions Act (FACTA) requires businesses to provide this information if the victim presents a police report. Merchants wouldn't release the records prior to FACTA.

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. [TransUnion](#), [Experian](#), and [Equifax](#) all have dispute information online.

Identity theft is not the only cause for credit report errors. A 2004 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.

- CheckRite - 1-800-766-2748
- ChexSystems - 1-800-428-9623 (closed checking accounts)
- CrossCheck - 1-800-552-1900
- Equifax - 1-800-437-5120
- International Check Services - 1-800-631-9656
- National Processing (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.

Contact the Federal Trade Commission

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. File a [complaint with the FTC](#) by contacting the FTC's Identity Theft Hotline 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: www.consumer.gov/idtheft

Mail Theft

Submit a [complaint](#) to the U.S. Post Office if you suspect your identity thief used your mail.

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.

Links

- [Federal Trade Commission](#)
- [Take Charge: Fighting Back Against Identity Theft](#)
- [Privacy Rights Clearinghouse](#)
- [FTD ID Theft Complaint Data - 2005](#)
- [FACTA - Fair and Accurate Credit Transaction Act](#)
- [Identity Theft Resource Center](#)
- [U.S. Dept of Justice -- Identity Theft and Fraud](#)
- [U.S. Postal Inspector Service](#)
- [Social Security Administration -- Identity Theft](#)
- [Identity Theft and Your Social Security Number](#)
- [Frequently Asked Questions on SSNs and Privacy](#)
- [Is Your Identity Adequately Protected?](#)
- [Most Misused SSN](#)

Computer Safety

- [OnGuardOnline](#)
- [Stay Safe Online - National Cyber Security Alliance](#)
- [GetNetWise](#)
- [Anti-Phishing Working Group](#)
- [TRUST-e](#)

Legislative Links

Search for current congressional legislation online at [Thomas Legislative Information](#).

- [Identity Theft Assumption and Deterrence Act of 1998](#)
- [Fair Credit Reporting Act](#)
- [FACTA - Fair and Accurate Credit Transaction Act](#)
- [Fair and Accurate Credit Transactions Act of 2003](#)
- [Identity Theft Penalty Enhancement Act](#)