PREVENTING ID THEFT 101

altana fcu
the better banking alternative

406.651.AFCU (2328)
www.altanafcu.org

The sponsoring editor for this book was Michelle Mielke, the editing supervisor was Loni Bienek, the designer was Amy Schmidt.

Preventing Identity Theft

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, change service providers for your cell phone, or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But an identity thief does.

How Identity Thieves Get Your Personal Information

1. They may steal your mail. They may take financial and credit card statements, credit card offers, new checks and tax information.
2. They may rummage through your trash. Called "dumpster diving," identity thieves may go through your trash, the trash of businesses, or public trash dumps.
3. They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM where you may enter or swipe your card.
4. They may steal your wallet or purse.
5. They may steal personal information they find in your home.
6. They may steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or "pretexting" by phone.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years — and thousands of dollars — cleaning up the mess the thieves have made of a good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit. Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity. The best way to avoid this mess is to take all the steps possible to prevent it before it occurs.

How Identity Thieves Use Your Personal Information

1. They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.

2. They may open new credit cards in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.

3. They may establish phone or wireless service in your name.

4. They may open a bank account in your name and write bad checks on that account.

5. They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

6. They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

7. They may buy a car by taking out an auto loan in your name.

8. They may get identification such as a driver's license issued with their picture, in your name.

9. They may get a job or file fraudulent tax returns in your name.

10. They may give your name to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

If Your Personal Information Has Been Lost or Stolen

Financial Accounts:

Close accounts, like credit cards and financial accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers for your password.

Social Security Number:

Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report too. An alert can help stop someone from opening new credit accounts in your name. Contact information for consumer reporting companies follows:

- **Equifax:** 1-800-525-6285; www.equifax.com; PO Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (1-888-397-3742); www.experian.com; PO Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790

Driver's License/Other Government-Issued Identification:

Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you've taken these precautions, watch for signs that your information is being misused (see next section).

If your information has been misused, file a report about the theft with the police, and file a complaint with the Federal Trade Commission as well.

Staying Alert

It is good to stay alert for possible signs of identity theft, like:

- Failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Receiving credit cards that you didn't apply for.
- Being denied credit or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.



Getting Your Credit Report – Free Annual Credit Reports:

The Fair Credit Reporting Act requires each of the nationwide consumer reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months.

To order your free annual report from one or all of the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281. The form is available at ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually. They provide free annual credit reports only through the website, phone number or mailing address listed above.

The Federal Trade Commission (FTC) advises consumers who order their free annual credit reports online to be sure to correctly spell www.annualcreditreport.com, or link to it from the FTC's website (ftc.gov/credit) to avoid being misdirected to other websites that offer supposedly free reports, but only with the purchase of other products. While consumers may be offered additional products or services while on the authorized website, they are not required to make a purchase to receive their free annual credit reports.

What To Do Today

When it comes to identity theft, you can take certain steps to minimize your chance of becoming a victim.

- Place passwords on your credit card, financial, and phone accounts. 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.
- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.
- Ask about information security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

Maintaining Vigilance

- Don't give out personal information over the phone, through the mail, or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of financial institutions, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its web address, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.
- Treat your mail and trash carefully. Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the US Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.
- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and financial institution statements, expired charge cards that you're discarding, and credit offers you get in the mail. To opt out of receiving offers of credit in the mail, call 1-888-5-OPTOUT (1-888-567-8688). The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. *Note: You will be asked to provide your SSN which the consumer reporting companies need to match you with your file.*
- Don't carry your SSN card; leave it in a secure place.
- Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your health insurance company uses your SSN as your policy number, ask to substitute another number.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.
- When ordering new checks, pick them up from your financial institution instead of having them mailed to your home mailbox.

Computer Safety

You may be careful about locking your doors and windows, and keeping your personal papers in a secure place, but do you keep your computer safe? Depending on what you use your personal computer for, an identity thief may not need to set foot in your house to steal your personal information. You may store your SSN, financial records, tax returns, birth date, and financial account numbers on your computer. These tips can help you keep your computer — and the personal information it stores — safe.

- Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally virus protection software should be set to automatically update each week.

- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.

- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

- Use a secure browser — software that encrypts or scrambles information you send over the Internet — to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You can also download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password — a combination of letters (upper and lower case), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

- Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy — or if you can't understand it — consider doing business elsewhere.

A Special Word About Social Security Numbers

Your employer and financial institutions will need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general record keeping. If someone asks or your SSN, ask:

- Why do you need my SSN?
- How will my SSN be used?
- How do you protect my SSN from being stolen?
- What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business. The decision to share is yours.

Your Wallet Register

In case you would ever lose your purse or wallet, it's a good idea to record information on credit cards, department store and gas charge cards, and ATM and debit cards. Don't forget corporate credit cards. Please keep this document safe; it contains very sensitive data.

Driver's license number _____

DMV phone number _____

Card	Issuer	Card number	Phone number

Important Terms

Browser - an application program that provides a way to look at and interact with all the information on the World Wide Web.

Consumer Reporting Company - there are three major consumer reporting agencies: Equifax, Experian and TransUnion. They keep track of your credit records, and issue credit reports to those who have a legitimate reason for needing to know your credit history.

Credit Report - a credit report is a consumer's credit history prepared by a credit bureau and used by a lender in determining the consumer's creditworthiness. Credit reports are also used by potential employers and insurance agencies to determine risk.

Data Breach - a data breach is the unintended disclosure of information that compromises the security of personally identifiable information and can often lead to instances of identity theft.

Data Encryption - data encryption is the reversible transformation of data from the original version to a difficult-to-interpret format, as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Most web sites employ data encryption to protect your information during e-commerce.

Dumpster Diving - identity thieves rummage through trash looking for bills or other paper with your personal information on it.

Fair Credit Reporting Act (FCRA) - a United States federal law that gives everyone the right to see what the Consumer Reporting Agencies have on file in their credit report.

Federal Trade Commission (FTC) - an independent agency of the United States government. Its principal mission is the promotion of consumer protection and the elimination and prevention of anti-competitive business practices.

Firewall - an integrated collection of security measures designed to prevent unauthorized electronic access to a computer.

Hackers - individuals who generally gain access and exploit computer systems and networks without their owners' knowledge or consent.

Identity Theft - a crime in which a criminal obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to pose as someone else. The information can be used to obtain credit, merchandise, and services using the victims' name.

Mail Fraud - identity thieves steal your mail, which may include pre-approved credit card applications or any other information that will help them get credit in your name.

Opt-Out - notifying a financial institution, insurance company, Consumer Reporting Agencies, or any other company that sells your personal information that you do not want your information shared. This is your right, it is always free, and it protects you from unwanted junk mail and phone calls, not to mention identity theft.

Password - a series of characters that enables someone to access a file, computer or program.

Patch - an accumulation of fixes to a known problem or to a potential problem within the operating system or other supported software. A patch can also provide a new feature or an enhancement to a particular software release. A patch consists of files and directories that replace or update existing files and directories.

Personal Information - any data that can be used to identify an individual. Examples of personal information are: names and addresses, Social Security Numbers, driver's license numbers, employee ID numbers, mother's maiden names and account information, including financial accounts and credit accounts.

Phishing - identity thieves pretend to be financial institutions or legitimate companies and send spam or pop-up messages to get you to reveal your personal information.

Pretexting - identity thieves pretend to be financial institutions or legitimate companies and use the phone to get you to reveal your personal information.

Privacy Policy - a declaration made by an organization regarding its use of the personal information that you give it.

Skimming - identity thieves capture credit/debit card numbers by using a special data storage device when processing your card for a purchase or by attaching the device to an ATM where you may enter or swipe your card.

Spyware - software that secretly gathers information about a person or organization or is designed to take partial or full control of a computer's operation without the knowledge of its user.

Virus Protection Software - a utility that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.

Wipe Utility Program - securely overwrites all files and prevents them from being recovered. Use of a wipe utility program is recommended before you dispose of a computer.

Notes

Preventing ID Theft 101

The majority of the information contained in this book is from the Federal Trade Commission's publication on ID Theft. However, some of the information is based on the opinions of Capital Credit Union.

Revised: 2/09