Recovering from identity theft

The FACT Act helps ensure that all citizens are treated fairly when they apply for credit. It provides new national ID theft protections as well.

Before, identity theft victims had to call all their credit card issuers and the three major credit bureaus to alert them to crime. Now, credit bureaus will share identity theft complaints, and consumers will need to make only one call to receive advice, set off a nationwide fraud alert, and protect their credit standing.

The Act also allows active duty military personnel to place special alerts on their files when they are deployed overseas.

To help recover from identity theft:

- Contact all creditors, utilities, and financial institutions about fraudulent accounts and follow up each conversation with a letter. Close suspicious accounts and open new ones using new passwords and PINs (personal identification numbers). Don't use recognizable identifiers such as the last four digits of your SSN, your birth date, house number, and so on for passwords and PINs.
- File a report with your local police or the police where the theft took place. Get a copy of the report in case a creditor needs proof of the crime.
- File a complaint with the FTC at the Identity Theft Hotline, toll-free at 877-IDTHEFT (438-4338).
- Ask your creditors if they'll accept the FTC's ID Theft Affidavit. You can get one by calling the FTC at 877-IDTHEFT or at *www.consumer.gov/idtheft*. The affidavit allows consumers to report identity theft information to several companies simultaneously.
- If it appears that someone is using your SSN, contact the Social Security Administration to verify the accuracy of your reported earnings and your name. Call 800-772-1213 to check your Social Security statement.

Social Security Number Advice

You are required to provide your SSN for:

- Income tax records
- Medical records
- Credit bureau reports
- College records
- Loan applications
- Vehicle registrations

You can and may want to refuse to provide your SSN in these situations:

- As driver's license number (in most states)
- On personal checks
- Over the phone
- On club memberships
- On address labels
- As identification for store purchases/refunds
- As general identification

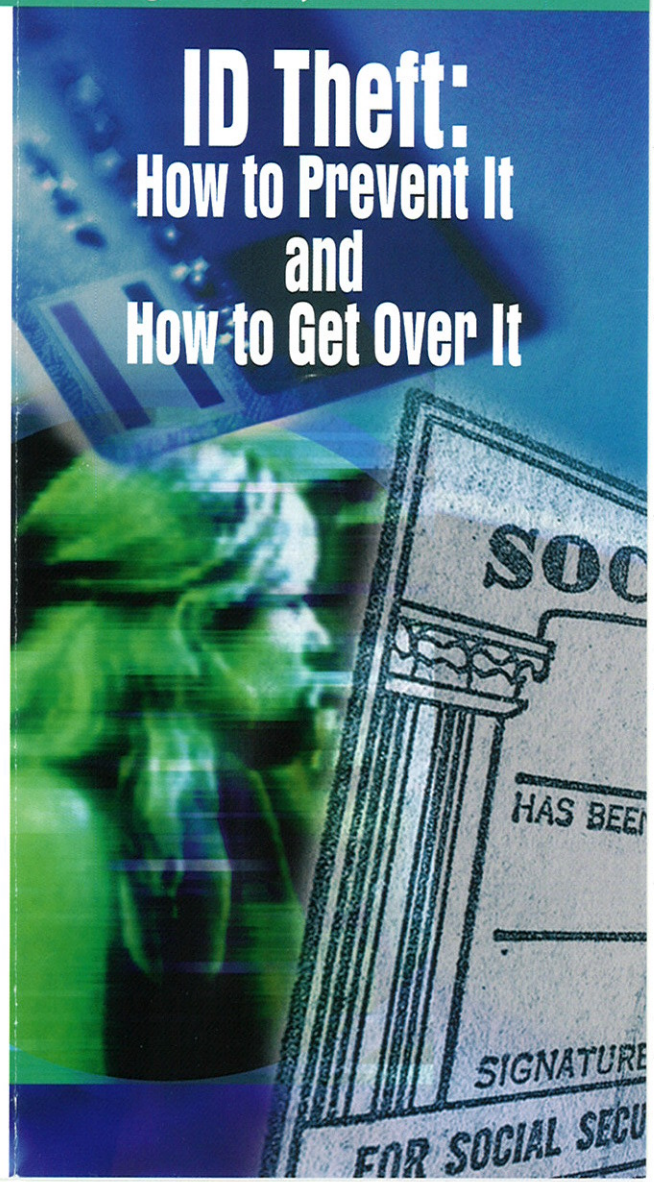
CUNA
Credit Union National Association
Personal Finance

AMERICA'S CREDIT UNIONS™

cuna.org
To order: 800-356-8010, ext. 4157
Stock No. 24209-PRO

Brought to You by Your Credit Union

ID Theft: How to Prevent It and How to Get Over It



Identity theft occurs when a thief obtains—and illegally uses—your identifying information, such as your Social Security number (SSN) or your credit card or checking account numbers, to open new credit accounts and apply for loans in your name.

If you're a victim, reclaiming your good name can take years and can be expensive. According to the Federal Trade Commission (FTC), the mean amount of fraud per victim was $5,720 in 2007.

An ID thief often is someone you know who strikes by redirecting mail, stealing sales receipts, or shoulder surfing—peeking over people's shoulders while they're at the ATM (automated teller machine). Technology just expands the opportunities.

Spoofing, spamming, and phishing

Identity thieves aren't only picking sales receipts and credit card offers out of trash cans to steal your information. They're using highly technical methods. They spoof, spam, and phish.

Spoofers create a replica of an existing Web page to fool a user into submitting personal, financial, or password data.

Make sure the Web sites you visit show a padlock on your browser window—the padlock signifies the use of SSL (secure sockets layer) technology. By convention, URLs (uniform resource locators) that require a safe connection start with *https:* or *s-http:*.

Spammers send unsolicited e-mail indiscriminately to multiple mailing lists, individuals, or newsgroups. These e-mails include advertisements, viruses, and hoaxes. Report spam by sending an e-mail to the FTC at *spam@uce.gov*.

Phishers create and use e-mails and Web sites—designed to look like e-mails and Web sites of well-known legitimate businesses, financial institutions, and government agencies—to deceive users into disclosing financial institution and account information or other personal data such as usernames and passwords.

Preventing identity theft

• Before revealing personal financial information, find out whom you're dealing with, how the information will be used, and if it will be shared with others.

• Only give your SSN when it's absolutely necessary (see box, next page). Ask if you can use another identifier, such as a driver's license, instead. And don't carry your Social Security card in your wallet unless you need it that day.

• Keep items with personal information in a safe place and either shred them or tear them up when you don't need them anymore. Dispose of checking/share draft copies and statements, receipts with a credit card imprint, insurance forms, expired credit cards, savings and investment account statements, and credit card offers the same way.

• Order a copy of your credit report from each credit-reporting agency every year. The Fair and Accurate Credit Transactions Act (FACT Act) of 2003 requires each major credit bureau to provide one free credit report annually to consumers who request a copy (call 877-322-8228, or visit *annualcreditreport.com*).

• Verify that your credit report is accurate and that it includes only activities you've authorized.

• Look over your credit card and credit union statements each month for unauthorized charges or suspicious activity.

• Photocopy financial cards and insurance cards you carry in your wallet (front and back) and keep copies in a safe place; if your wallet is lost or stolen, you can promptly and accurately report the loss.

• Consider the information you're supplying on entries to win a car, shopping spree, and so on. To win, information such as your age or income range usually is not necessary.

• Contact the U.S. Postal Service if you don't receive mail for a few days. You want to confirm that your mail—with, say all those credit card offers—hasn't been diverted by a thief filling out a change of address form in your name.

Here is a list of the three major credit bureaus:

		Request a copy of credit report	Fraud units
• Experian	*experian.com*	888-397-3742	888-397-3742
• Equifax	*equifax.com*	800-685-1111	800-525-6285
• TransUnion	*transunion.com*	800-888-4213	800-680-7289

Useful Resources:

ID Theft Resource Center
idtheftcenter.org

FTC: National Resource for ID Theft
www.consumer.gov/idtheft/

Information about preventing identity theft, avoiding sweepstakes scams, and being a smart catalog shopper:
dmachoice.org/consumerassistance.php

Common scams:
staysafeonline.info/basics/pharming_tips.html

FiscalFacts

Up-to-date Financial Information and Consumer Alerts

A service of NuUnion CREDIT UNION

Protecting Yourself From Identity Theft

How to protect your identity

Identity theft is the fastest growing crime in America. It occurs when someone obtains your personal information (Social Security Number, credit card number, etc.) and uses it to fraudulently apply for credit, make purchases, or withdraw money from your accounts. It seriously jeopardizes your finances and credit standing.

Follow these steps to minimize risk:

- Don't routinely carry social security card, credit cards you rarely use, or any other non-essential items that contain personal information. Limit the number of credit cards you have and cancel any inactive accounts. Any one of these can give an identity thief access to information and personal data. For example, with your Social Security Number, an identity thief can apply for a credit card or driver's license, access your personal records, and assume your identity.
- Never leave your purse or wallet unattended at work, at restaurants, at health fitness clubs, in your shopping cart, or at parties. Never leave your purse or wallet in open view in your car, even when locked.
- When someone contacts you over the phone or internet, never give them any credit card, financial institution, or social security information.
- When you contact a company, make sure you know the company and the representative before providing any personal information.
- Destroy all checks immediately when you close a checking account. Destroy or keep in a secure place any courtesy, cancelled, or unused checks that your financial institution or credit card company mails to you. Immediately report lost or stolen checks to your financial institution.
- Shred all your important papers that you no longer need, especially pre-approved credit applications that you receive in your name and other financial information that could provide access to your private information. Shred your credit and debit card receipts, too.
- Carefully monitor financial statements (bank, credit union, credit card, investment, etc.) so that you may detect any unauthorized charges or withdrawals as soon as possible. Immediately report unauthorized use to your financial institution or credit card company.
- If regular bills fail to reach you, contact the company to find out why.
- Memorize your passwords and personal identification numbers (PINs). Never keep your PIN with your ATM/debit or credit cards and never give out your PIN to anyone. Shield the ATM keypad when entering your PIN. Always request your debit and credit card receipts and/or carbons, and take your receipts with you.
- Photocopy or list all credit and identification cards you carry with you. Include both the front and back as well as corresponding customer service phone numbers so you can quickly contact the issuers to inform them of lost or stolen cards. Keep this information in a secure place (not your wallet or purse).
- Don't put outgoing mail in your mailbox. Take the time to drop it into a postal service box (especially bill payments). Identity thieves can obtain personal information by stealing outgoing mail.

- Order a copy of your credit report and check it for accuracy. You can do this online by visiting NuUnion.org and clicking on Education. The law requires each bureau to provide you with a free copy of your credit report once every 12 months if you request it.

Although there's no foolproof way to protect yourself from identity theft, these safeguards make it more difficult for an identity thief to steal your personal information. It's worth the effort to take the precautions.

What to do after identity theft?

If you suspect that you're a victim of identity theft (i.e., you notice unauthorized transactions on your credit card or financial institution statements), you need to act as quickly as possible to minimize the damage to your finances and your credit standing.

Here are the steps to take:

- Immediately contact every financial institution you do business with to inform them of your situation and to secure your accounts.
- Contact all three major credit bureaus to report the theft:

Equifax 800.525.6285
P.O. Box 74024
Atlanta, GA 30374

Experian 888.397.3742
Consumer Fraud Assistance
P.O. Box 949
Allen, TX 75013-0949

TransUnion 800.680.7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92634

- Ask for a Fraud Alert to be placed in your file.
- Ask for a Victim's Statement that tells creditors to call you before opening a new account or changing an existing one.
- Request and examine a copy of your credit report (this copy should be free). Look for any inquiries unknown to you and report any discrepancies in writing to the credit bureau immediately.
- Call your credit card companies and other creditors to alert them that you've been the victim of identity theft. Ask for a new card and account number. You can limit your liability by reporting unauthorized use as promptly as possible. Follow up with a written notification to your credit card companies and creditors.
- Report the theft to the police in your community immediately and keep a copy of their report for future reference. If you know where your identity was stolen, contact the police in that jurisdiction as well.
- Be prepared to fill out affidavits of forgeries for financial institutions, credit grantors, and recipients of stolen checks. They are joint victims with you and may suffer a financial loss.
- If your mail was stolen, contact your local U.S. Postal Inspection Office (the postal service law enforcement division). To locate your nearest U.S. Postal Inspection Office, call 800.275.8777.
- Report the theft to the Federal Trade Commission at 877.438.4338.
- If someone is using your Social Security Number, contact the Social Security Administration's Office of Inspector General at 800.269.0271.
- Keep a record of all related correspondence and conversations with individuals at your financial institutions, credit bureaus, and other agencies.

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you think you've become a victim of identity theft, it is crucial that you act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation. Identity theft, while disturbing, doesn't have to be devastating if you take the right steps as quickly as possible.

Call immediately if you suspect unauthorized use of your accounts. We're here to help.

NuUnion
CREDIT UNION

888.267.7200 • NuUnion.org

850 (06/06)

NuUnion
CREDIT UNION

Helpful Resources

Victim Advice and Assistance

Privacy Rights Clearinghouse
E-mail: prc@privacyrights.org
Website: www.privacyrights.org

Federal Trade Commission (FTC) Identity

Phone: 877.438.4338
Website: www.consumer.gov/idtheft

Direct Marketing Association

Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735

Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735

To get a free credit report:

Website: www.annualcreditreport.com
Phone: 877.FTC.HELP
Mail: Standardized request form (available online) to Box 105281, Atlanta, GA 30348-5281

Consumers are allowed one free report per year from each of the agencies

Social Security Administration

Data Operations Center
P.O. Box 7004
Wilkes Barre, PA 18767

Report Fraud: 800.269.0271
Request Report: 800.772.1203

Helpful Websites

www.identitytheft.org
www.privacyrights.org
www.consumer.gov/idtheft
www.ssa.gov
www.bos.frb.org/consumer/identity/index.htm
www.michigan.gov/ag
www.annualcreditreport.com

NuUnion Credit Union

Phone: 517.267.7200 or 888.267.7200
Website: NuUnion.org
South Lansing Branch: 438 East Edgewood, Branch Sales Manager Carolyn Murray
Frandor Branch: 300 North Clippert, Branch Sales Manager Bill Lantzy