

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

Social Security Number

You are required to provide your SSN for:

- Credit unions
- Income tax records
- Medical records
- Driver's license and your 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

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 (38-7348) or at ftc.gov.
- Ask your creditors if they have created an FTC's ID Theft Affidavit. You can get the affidavit from the FTC at 877-IDTHEFT or www.ftc.gov/idtheft. The affidavit allows consumers to report identity theft information to several companies simultaneously.
- If you suspect 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.



cuna.org
To order: 800-356-8010, ext. 4157
 Stock No. 24209-PRO
 © 2009 Credit Union National Association Inc.,
 the trade association for credit unions in the U.S.

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 a 2009 Identity Fraud Survey Report by Javelin Strategy and Research, individual victims said perpetrators stole, on average, \$4,849 in cash, goods, or services in 2008.

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. Technology just expands the opportunities.

Spoofing, spamming, and phishing

Identity thieves aren't only poisoning sales receipts and credit card offers; they're also stealing your information. They're using highly technical methods. They spoof, spam, and phish.

Spoofers create a duplicate of an existing Web page and use it to solicit 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 sensitive financial information, find out whom you're dealing with. How the information will be used, and how it will be shared with others, is important to know. Don't give out your SSN when it's absolutely necessary (see [page 10](#)). 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 know that your mail—with, say, all those credit card offers—hasn't been diverted. Look for a notice of change of address form in your mailbox.

Useful resources:

ID Theft Resource Center
idtheftcenter.org

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

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

Common scams
staysafeonline.org

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