

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.org
To order: 800-356-8010, ext. 4157

Stock No. 24209-PRO
© 2005 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 the Federal Trade Commission (FTC), the average consumer spends more than \$1,000 to clean up the damage done by identity thieves opening new accounts.

Traditionally ID thieves have struck by redirecting mail, stealing sales receipts, and shoulder surfing—peeking over people's shoulders while they're at the ATM (automated teller machine). Technology expands their opportunities.

Spoofting, 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 near the bottom of your browser window—the pad-

lock 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 uce@ftc.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 invest-

ment 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, phased in by region, to consumers who request a copy (call 877-322-8228, or visit www.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/

FTC brochure: Take Charge: Fighting Back Against Identity Theft
ftc.gov/bcp/online/pubs/credit/idtheft.htm