TrueCore
FEDERAL CREDIT UNION

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

RECOVER FROM IDENTITY THEFT

The FACT Act helps ensure that all citizens are treated fairly when they apply for credit. It provides national ID theft protections as well. Credit bureaus now share identity theft complaints, and consumers need to make only one call to set off a nationwide fraud alert. The Act also allows active duty military personnel to place special alerts on their files when they are deployed overseas.

Follow these steps to recover from identity theft:

- Contact all creditors, utillties, 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.
- 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 requests proof of the crime.
- File a complaint with the FTC at the Identity Theft Hotline, toll-free at 887-IDTHEFT or at *ftc.gov.*
- Ask your creditors If they'll accept the FTC's ID Theft Affidavit. You can get one by calllng the FTC at 877-IDTHEFT or at *consumer.gov/idtheft.* The affidavit allows consumers to report identity theft information to several companies simultaneously.
- If you think someone is using your SSN, contact the Social Security Administration at 800-772-1213 to verify the accuracy of your reported earnings and your name.

REDUCE YOUR RISKS- START TODAY

Personally, you can greatly diminish your own risk to identity theft. Here are thee simple steps to get you started:

1.) Switch to strong passwords. It's worth your time to update all your passwords to contain upper and lower case letters, numbers, and symbols. Dictionary words are easily hacked (as Britney Spears and Barack Obama found out when their Twitter accounts were compromised). Avoid recognizable identifiers such as the last four digits of your SSN, your birth date, house number, and so on for passwords and PINs. One idea is to memorize a sentence, using the first letter of each word -including numbers and symbols -as your password (e.g., "My #1 dog is a Lab/Poodle mix" becomes M#1diaL/Pm).

2.) Refuse requests for personal Information. Decline phone and email requests for personal information or your credit card number. They may be scams. For example, the credit union will not call or e-mail you asking for your SSN or birthdate -we already have this information. Instead, contact the institution directly.

3.) Order your free credit reports. Request a copy of your credit report and review for unauthorized accounts. 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*).

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

IDENTITY THREATS

An ID thief can strike by pocketing a wallet or phone, dumpster diving, redirecting mail, stealing sales receipts, or shoulder surfing - peeking over people's shoulders while they're at the ATM. Technology just expands the opportunities.

- **Phishers** create and use e-mails and websites - designed to look like those of legitimate businesses - to deceive users into disclosing information. To avoid, don't click on the links. Instead, contact the organization directly.
- **Pharmers** secretly install (or plant) a malicious program in your computer to hijack your web browser. Pharming crimeware misdirects users to fraudulent sites and captures what you enter, such as passwords or account information. To avoid, turn on your firewall, accept security patch updates, and install virus software protection.
- **SMiShers** phish via cell phone text messages. The message typically alerts the user of a need for immediate action with a link to a phony site. Again, instead of replying to these messages or following links, contact the organization directly.

Protecting your personal information and your accounts is our top priority. Your credit union has implemented layers of online security to guard your deposits, and we continually evaluate new methods to defend against hackers. For example, when you make an electronic transaction, you may be asked to answer a security question or re-enter a password -it's just another layer of protection for your accounts. Still, if you ever encounter suspicious activity on a credit union account, contact us immediately, so that your liability for any unauthorized transactions may be limited.

Request a free credit report from AnnualCreditReport.com or call 877-322-8228. If you find suspicious activity, contact one of these credit bureaus.

	Information	Fraud Units
Experian - experian.com	888-397-3742	888-397-3742
Equifax - equifax.com	800-685-1111	888-766-0008
TransUnion - transunion.com	800-888-4213	800-680-7289

TrueCore FEDERAL CREDIT UNION
215 Deo Drive, Newark
740-345-6608 • 800-333-2465

Credit Union National Association
CUNA
cuna.org

SOCIAL SECURITY NUMBER ADVICE

You are required to provide your SSN for:

- Credit unions/banks
- Income tax records
- Medical records
- Credit bureau reports
- College records
- Loan applicatlons
- Vehicle registrations

You can refuse in these situations:

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

PREVENT IDENTITY THEFT

- Carry only essential cards and ID. Photocopy financial 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.
- Lock down your cell phone to protect personal information should it be stolen or lost.
- Only give your SSN when it's absolutely necessary, and do not carry your Social Security card in your wallet unless you need it that day.
- Shred personal and financial records before discarding.
- Look over your credit card and credit union statements each month for unauthorized charges or suspicious activity.
- Contact the U.S. Postal Service if you don't receive mail for a few days. You want to confirm that your mail hasn't been diverted by a thief filling out a change of address form in your name.