Preventing Identity Theft

Here are a few basic steps you can take to avoid becoming a victim of identity theft and pretext calling.

Identity theft is the fraudulent use of a person's personal identifying information.
Often, identity thieves will use another person's personal information, such as a Social Security number, mother's maiden name, date of birth, or account number to open fraudulent new credit card accounts, charge existing credit card accounts, write share drafts, open share accounts, or obtain new loans.
They may obtain this information by:

- Stealing wallets that contain personal identification information and credit cards.
- Stealing credit union statements from the mail.
- Diverting mail from its intended recipients by submitting a change of address form.
- Rummaging through trash for personal data.
- Stealing personal identification information from workplace records.

Intercepting or otherwise obtaining information transmitted electronically.

How Can Your Credit Union Help?

Credit unions often offer their members identity theft protection for their accounts, as well as resources to help recognize and prevent identity theft. Ask your representative for more information.

Steps to Protect Your Privacy

Do not share personal information, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet, unless you initiated the contact or know with whom you are dealing.

Store personal information in a safe place and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away.

Protect your PINs and other passwords. Avoid using easily available information such as your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, as identity thieves can use this information to access your accounts.

Carry only the minimum amount of identifying information and number of credit cards that you need.

Pay attention to billing cycles and statements. Contact the credit union if you do not receive a monthly bill. It may mean that the bill has been diverted by an identity thief.

Check account statements carefully to ensure all charges, share drafts, or withdrawals you authorized.

Guard your mail from theft. If you have the type of mailbox with a flag to signal that the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.
Consumers are entitled to one free credit report from each credit reporting bureau annually.

If you prefer not to receive pre-approved offers of credit, you can opt out of such offers by calling: (888) 5-OPT-OUT. (888-567-8688)

If you want to remove your name from many national direct mail lists, send your name and address to:

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

If you want to reduce the number of telephone solicitations from many national marketers, send your name, address, and telephone number to:

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

IDENTITY THEFT PROTECTION SERVICES

Identity theft protection services can help you monitor your accounts. They can place fraud alerts or freezes on your credit reports or remove your name from marketing mailing lists. Many people find it valuable and convenient to pay a company to keep track of their financial accounts, credit reports, and personal information. Other people choose to do this on their own for free. Before you pay for a service, evaluate it and its track record before you pay any fees.

Can a Monitoring Service Prevent Identity Theft?

Identity theft protection companies may help you:

- "**lock**," "**flag**," or "**freeze**" your credit reports

place a fraud alert or credit freeze on your reports

- renew or update your alerts or freezes automatically

An identity theft victim can place a fraud alert or renewal for free.

Some companies, including consumer reporting agencies, offer subscriptions to credit monitoring services. These services track your credit report, and generally send you an email about recent activity, like an inquiry or new account. The more frequent or more detailed the report, the more expensive the service.

Some companies offer services to help you rebuild your identity after a theft. Typically, you give these services a limited power of attorney, which allows them to act on your behalf when dealing with consumer reporting agencies, creditors, or other information sources.

Many companies offer additional services, including removing your name from mailing lists or pre-screened offers of credit or insurance, representing your legal interests, “guaranteeing” reimbursement in the event you experience a loss due to identity theft, or helping you track down whether your personal information has been exposed online.

Frauds and Scams, Be on the alert & stay informed.

In this section, NCUA reports on frauds and scams aimed at credit union members. You can view alerts on recent fraud activity, and fraud resources that will help you stay informed.

Cyber Crime

Anyone who believes they have been a target of a cyber crime should immediately contact their financial institutions and promptly report it to the Internet Crime Complaint Center’s (IC3) website at www.ic3.gov. The IC3’s complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The IC3 also uses complaint information to identify emerging trends and patterns.

The IC3 is a joint effort of the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA).

Methods used to steel you personal information:

Phishing

Beware of Phishing! Don’t click on links in e-mails that ask for personal information. Never open unexpected attachments. Delete suspicious messages, even if you know the source.
Phishing is when internet fraudsters impersonate a business in an attempt to trick you into giving out your personal information, such as usernames, passwords, and credit card details. Legitimate businesses don’t ask you to send sensitive information through insecure channels.
For example, a fraudulent email may state that NCUA will add money to the member's account for taking part in a survey. The link embedded in the message directs members to a counterfeit version of NCUA's website with an illicit survey that solicits credit card account numbers and confidential personal information. NCUA will never ask credit union members or the general public for personal account or personally identifiable information as part of a survey.

SMishing

The term SMishing is a combination of “SMS” and phishing. SMishing uses cell phone text messages or SMS (Short Message Service) to deliver a message in order to get you to divulge your personal and financial information. The method used to obtain information in the text message may be a web site URL, however it has become more common to see a phone number that connects to an automated voice response system.

Unsolicited Text Messages

Unsolicited text messages sent to cell phones urge the recipient to call a number provided for information about account discrepancies and then solicits individual account information and pin numbers. Cell phone users should be wary of unsolicited text messages. Such messages should be deleted and all deleted text messages should be removed, if possible, as the perpetrators have been known to use Spyware1 in conjunction with their text message solicitation.

Vishing

The term vishing is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations, are known to the telephone company, and are associated with a bill-payer. The victim is often unaware that voice over Internet Protocol (VoIP) allows for caller ID spoofing thus providing anonymity for the criminal caller. Rather than provide any information, the consumer should contact their financial institution or credit card company directly to verify the validity of the message using contact information they already have in their possession (i.e. do not use contact information provided in the suspicious message).

Create an ID Protection Strategy

As you work on creating an identity theft protection strategy to keep your personal and financial information secure, consider these common mistakes that could make you an easy target for an identity thief:

- Letting mail and financial statements pile up around the house;
- Carrying all of your credit and bank cards in your wallet at the same time;
- Creating passwords that contain your name, birth date, your pet's name or other information that could easily be found or guessed;
- Using the same password for multiple online accounts, such as your email, online banking account or favorite shopping website;
- Sharing the passwords to your smartphone, email, social media networks and other online accounts with others — even your family and friends.
- Using the word "password," or the numbers "12345678" as the password for your online accounts.

Never use your birthday, your name or the word "password" as a password for any online account.