

# AVOIDING FINANCIAL SCAMS

- **Pay attention to your billing cycles:** Contact creditors if you don't receive your bills on time – this could be a sign that your account has been taken over by an identity thief.
- **Secure personal information in your home:** Keep identification cards, passports and account numbers in a secure place in your home. Shred all personal information before throwing it away, including credit card offers.
- **Avoid impossible claims:** Be careful of deals that are “too good to be true” or are “good today only.”
- **Read the small print:** Get all promises in writing and read all paperwork before paying any money or signing any contracts.
- **Free means free:** Reject any offer that requires you to pay to get a gift or something that's “free.”

**If you suspect your credit union account has been compromised, contact us immediately. To report a financial scam, contact the Federal Trade Commission at:**

[www.ftc.gov](http://www.ftc.gov)

ID Theft Hotline 1-877-ID THEFT (438-4338)

Report Fraud 1-877-FTC HELP (382-4357)



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2007 National Association of Federal Credit Unions.

SF85-1107



**How to protect your money  
and your good name**

More than 30 million Americans have fallen victim to identity theft or other financial scams at a cost of billions of dollars, and the toll is mounting. As your credit union, we want to help you avoid becoming a victim. With a few simple precautions and a healthy dose of common sense, you can protect your finances and your good name from financial scammers.

## COMMON FINANCIAL SCAMS

It's important to be aware of the ways in which scammers try to separate you from your money. Here are some of the most common financial schemes:

### IDENTITY THEFT

Identity thieves use your personal information, such as your Social Security number or credit card number, to open new accounts and run up high bills in your name.

### CHECK FRAUD

Criminals use counterfeit checks drawn on your bank account. Thieves typically obtain your account information by stealing a blank check of yours, getting old financial documents from your trash, or removing bills or other financial information from your mailbox.

### CHECK SCAMS

A stranger seeks your help cashing a large check, offering to let you keep most of the cash if you agree to send a smaller portion back. When the check bounces, you are liable for the entire amount plus fees – and you're also out any money the thief talked you into sending back.

### LOTTERY OR SWEEPSTAKES SCAMS

A scammer sends a letter or e-mail claiming you've won a lottery or cash prize. They send a fake check for part of your winnings and ask you to send them money to cover the "taxes" to get the rest of the money.

### PHISHING

Scammers send an e-mail or telephone you, claiming to be from your financial institution, a retailer or government agency, and try to trick you into providing your financial or personal information. **Remember, your credit union will never contact you for personal information, such as your account or Social Security numbers.**

### PHARMING

You get a bogus e-mail that appears to be from your credit union, credit card company or other financial services provider. The e-mail directs you to click on a link to an official-looking Web site, where you're asked to provide personal information. Thieves then "harvest" your information to gain access to your financial accounts.

### OVERPAYMENT SCAMS

Scammers buy merchandise you advertise online or in the newspaper, and send a fake check or money order for more than the amount advertised. They then ask you to send back the excess money.

### PHONE FRAUD

A scammer pretends to be selling goods or investments, or requests donations to unregistered charities. The caller attempts to obtain financial or credit card information.

### CREDIT CARD FRAUD

An identity thief uses your credit card, or opens a new credit card account in your name, to purchase merchandise. You may not find out until your credit is ruined due to large unpaid credit card bills.

## HOW TO PROTECT YOURSELF

Stay smart: Your best defense is knowledge. By taking a few precautions, you can help fight fraud and avoid unnecessary worry and expense. Here are some tips to help you protect your good name, based on Federal Trade Commission recommendations:

- **Know who you're dealing with:** Do business only with companies that plainly provide their name, street address and phone number. You can also verify any information on a company's Web site with a company representative.
- **Visit the organization's Web site the safe way:** Type in a company's URL, rather than clicking on a link provided in an e-mail you receive. If you have suspicions about any e-mails you receive, call the company's representative by phone for verification.
- **Protect your personal information:** Don't give out personal information on the phone, through the mail or over the Internet, unless you've initiated the contact.
- **Use passwords wisely:** Help protect your credit union, credit card and utility accounts by placing a password on them whenever possible. Avoid using easily available information, like your mother's maiden name or your birth date, as your password.