STOP THESE BAD HABITS:

- Don't leave your cards unsigned.
- Don't disclose your PIN to anyone—including to someone who claims to represent the card issuer or financial institution—who telephones or e-mails you.
- Don't write your PIN on your card.
- Don't respond to any type of e-mail or phone request asking for your personal or financial information. The people at your credit union would never ask you for this—we already have it on file.
- Don't allow your card to be out of your sight or allow cashiers or anyone else to enter your PIN for you, even if they are helping you with the transaction.
- Don't allow a sales clerk to write your card number on a personal check as identification.
- Don't lend your cards to anyone or leave them unsecured and unattended anywhere, including your car (even if locked) or at work.
- Don't discard paper statements in trash cans or leave them where others can get at them.
- Don't let your mail pile up in an unsecured mailbox when you're traveling.
- Don't travel with just one card. If one is tainted by fraud, you'll need a backup.
- Don't count your money at the ATM.

Providing your personal and financial information to anyone can lead to ID theft and phishing attacks. Know whom you're dealing with. For more information about these exposures, contact your credit union.

When it comes to card safety, if you don't practice good habits, you'll pay. The good news is, practicing good habits goes a long way toward keeping you and your cards safe.

ID theft resources

ID Theft Resource Center
idtheftcenter.org

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

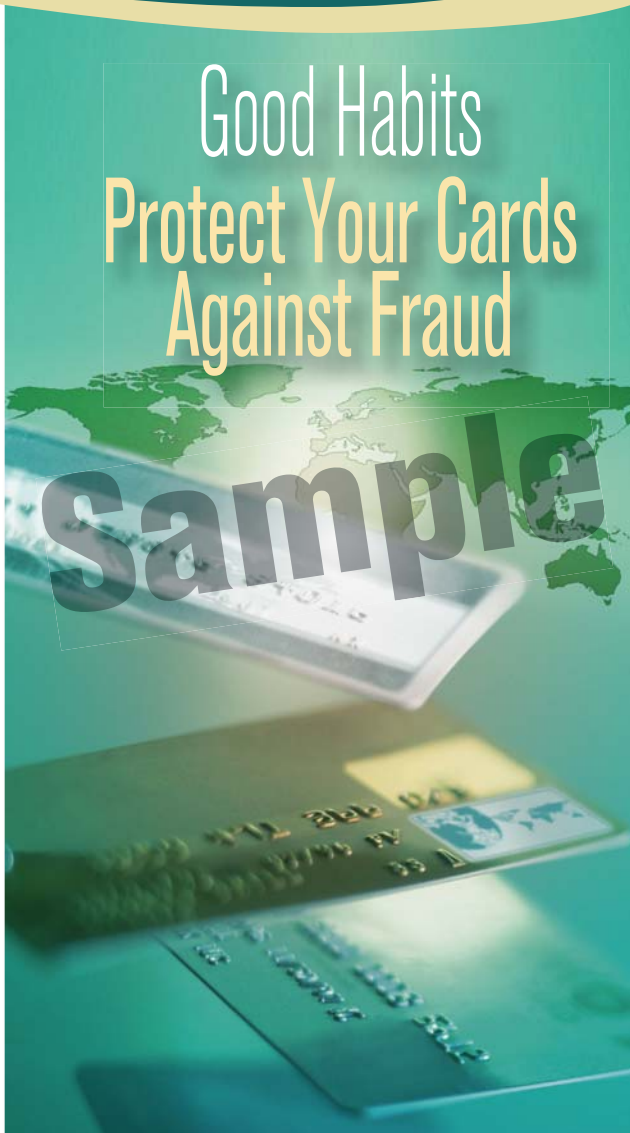
FTC brochure: Take charge: Fighting Back Against Identity Theft at *ftc.gov* search "take charge"

CUNA
Credit Union National Association
Personal Finance

America's Credit Unions

Stock No. 27319-PRO *cuna.org*

Good Habits
Protect Your Cards Against Fraud



Credit and debit card fraud statistics are up, and much of the fraud comes from criminal activities we can't control. But safeguarding your cards—and identity—from the risk of exposure starts with keeping constant control of your cards, card numbers, and any other details about your financial information.

"Paperless" cash is convenient, accepted almost everywhere, and, in proportion to the volume in use, very safe. But with convenience comes risk.

At the credit union, we're proud of the measures we take to help protect your cards. But we all need to be responsible and aware of actions that will minimize risk and keep our cards safe.

Make good habits and stop bad ones to minimize your card risk.

		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

PRACTICE THESE GOOD HABITS:

- **Sign your cards** with permanent ink as soon as you receive them.
- If your card has a PIN (personal identification number), memorize it. **Skip easily recognizable PINs** such as the last four digits of your Social Security number or phone number.
- **Routinely check your credit report for errors and unauthorized accounts.** Each major credit bureau must provide one free credit report annually to consumers requesting a copy: *annualcreditreport.com*, 877-322-8228.
- **Delete urgent e-mails requesting personal information.** This is commonly known as phishing. Phishers use authentic-looking e-mail to lure people into fake Web sites to obtain personal information and commit ID theft.
- **Carry only cards you're going to use.** Leave all other cards in a safe place at home , lessening the risk of theft.
- **Install anti-virus and anti-spyware software** on your computers, and turn on firewalls.
- **Switch to e-statements, and pay your balance online,** preventing thieves from stealing account information from your mailbox.
- **Before traveling, notify your card issuer** of the location and time frame to account for changes in your card use ("out of pattern" purchases).
- **Review card transactions** carefully as soon as you receive your statement.
- **Shred statements** unless you need them for proof of purchase, warranty authorization, or tax purposes.
- If you have online access to your statement, **review the account frequently** for any suspicious activity.
- Make sure online shopping sites show a closed **padlock in the bottom browser window frame**—outside the vendor Web site window.
- **Follow news about fraud** as it evolves with technology; those changes can affect you.
- When using an ATM (automated teller machine), **shield the screen and keypad** with your body to prevent others from seeing your PIN.
- **Inspect the ATM to identify any tampering** of the machine. Crooks can install devices to capture your information—commonly known as skimming.
- **Be cautious of someone contacting you**—in the guise of financial institution employees—advising you of unusual activity. Call your financial institution, at a number you'll find on your statement, for verification.
- **Report card loss** to your card issuer immediately.
- **Report your card fraud to the authorities.** If a suspect is identified, press charges.