

IF YOU BECOME A VICTIM

If you suspect that your personal information has been compromised and you are a victim of identity theft, follow these three basic steps:

1. Contact the fraud department of each of the credit bureaus listed below and advise them you are a victim of identity theft.
2. Contact the Credit Union and other financial institutions you do business with — including credit card issuers as soon as possible. Advise them of possible criminal activity. Close out any accounts that you believe have been tampered with or opened fraudulently.
3. File a police report with your local police where the identity theft took place.

HELPFUL NUMBERS AND WEB SITES:

Credit Bureaus

Equifax (800) 525-6285

Experian (888) 397-3742

Trans Union (800) 680-7289

Lost or Stolen Credit Cards and Check Card

Visa Check Card

(520) 794-8341 (800) 253-8245

Visa/MasterCard (800) 449-7728

Social Security Office (Fraud Hotline)

(800) 269-0271 www.ssa.gov

Federal Trade Commission (FTC) Identity Hotline

(877)-IDTHEFT (438-4338)

www.consumer.gov/idtheft

Hughes Federal Credit Union

(520) 794-8341 (800) 253-8245

www.hughesfcu.org

Hughes Federal Credit Union

P.O. Box 11900
Tucson, AZ 85734-1900



PROTECT YOUR GOOD NAME FROM IDENTITY THEFT



HOW TO KEEP YOUR PERSONAL INFORMATION SAFE AND SECURE AND PREVENT FRAUD



Hughes
Federal Credit Union

Yours for the asking™

PROTECT YOUR FINANCIAL IDENTITY

Despite your best efforts to protect your personal information, it only takes a few seconds to become a victim of financial fraud. But by managing your personal information wisely and cautiously you can guard against identity theft. Below are just some of the ways identity thieves can get your personal information:

- Steal your purse or wallet with credit cards and personal information.
- Steal your mail, bank and credit card statements, pre-approved offers, new checks and tax information.
- Submit a “change of address form” to divert mail to a new location.
- Rummage through trash to obtain personal information.
- Stealing information from places you may do business with.
- Phone calls from individuals posing as financial representatives to obtain information.
- Steal personal information off your personal computer.

MINIMIZE YOUR RISK

You may not be able to prevent identity theft entirely, but here are a few tips to help minimize your risk:

- Examine your financial statements and reconcile them monthly. Verify credit, debit and ATM receipts. Contact the appropriate company for discrepancies between your records and monthly statements.
- Keep receipts and duplicate check copies in a safe place.
- Shred unused checks from closed-out accounts and credit cards that are expired or not in use.
- Do not mail personal checks, bill payments or anything with your personal information on it from your home mailbox –or community mailbox. Use a secure mailbox such as a post office or a mailbox you *know* is secure.
- Keep your purse or wallet safe. Thieves often target unattended vehicles, unlocked office drawers, and health club locker rooms.
- Memorize your personal identification number (PIN). Never write it down or keep it with your card(s). Do not give it to anyone, not even family members.
- Never give personal information over the phone unless you have initiated the call.

- Be aware as to when your financial statements are due to arrive in the mail. If they’re late, contact the Credit Union or issuer.
- And, it’s a good idea to review your credit bureau reports once a year from the three credit bureau agencies (Equifax, Experian, and Trans Union).

PROTECT YOURSELF FROM ONLINE FRAUD

The Credit Union uses commercial strength technology when it comes to online or electronic security. However identity fraud can occur when consumers do not take precautions concerning electronic transactions. The following tips can help you keep your computer and your personal information safe.

- If you doubt the security of an online vendor, order items by phone. Look for the “lock” icon on the browser’s status bar to be sure your information is secure during transmission.
- If you email the Credit Union, use the secure email form located at the bottom of our Web site (www.hughesfcu.org).
- Update your virus protection software regularly.
- Do not download files sent to you by strangers.
- Use a firewall program, especially if you use a high speed Internet connection like cable, DSL, or T-1.
- Use a secure browser-software that encrypts or scrambles information you send over the Internet to guard the security of your online transaction.
- Try not to store financial information on your laptop, but if you do use a strong password and do not use the automatic log-in feature.
- Before you dispose of a computer, be sure to delete personal information. See: *Clearing Information From Your Computer’s Hard Drive* (www.hq.nasa.gov/office/oig/hq/harddrive.pdf).
- Look for Web site privacy policies. They answer questions about maintaining accuracy, access, security and control of personal information collected by the site.

For more information, see: *Site-Seeing on the Internet: A Traveler’s Guide to Cyberspace* (www.ftc.gov).