

Helpful Security Precautions to Help You Assist Your Members with Protecting Their Accounts

- ✓ Caution! Mail and telephone solicitations bring many tempting offers, but not all are legitimate. Be especially careful about deals that sound too good to be true, and don't give callers your card number unless you want them to charge your account.
 - Be wary of high-pressure sales tactics, especially if the sale must be done now.
 - Record the name, address, and phone number of the firm.
 - Obtain names of other customers who can supply references.
 - When in doubt, consult the Better Business Bureau or the U.S. Postal Inspection Service.
 - Ask questions. The fewer questions the telemarketer can answer, the less likely that it is a legitimate business.
- ✓ Memorize your personal identification number (PIN). Don't write it down in your wallet or on the back of the card. Don't designate the same PIN number for all your cards, and don't designate a number such as your birth date, that can be found easily in your wallet.
- ✓ Never disclose your PIN to anyone. No one from a financial institution, the police, or a merchant should ask for your PIN. You are the only person who should know it. If someone calls you claiming to be a bank representative and asks for your PIN number, don't give it to them. Report it to your credit union and the police.
- ✓ When selecting a PIN, always avoid the obvious – your name, telephone number, or date of birth, or any combination.
- ✓ When your card has become stuck inside of the ATM machine, be suspicious of anyone offering their help, even if they appear to be a credit union security officer. Criminals can obtain your PIN by several means (shoulder surfing or straightforward questioning), then retrieve your jammed card from the ATM and use it to withdraw funds.
- ✓ Protect your cards as if they were cash. Never leave your cards unattended – at work, at your sports club, in a shop, or in a doctor's office.
- ✓ Don't leave your credit cards in your car's glove compartment. An alarmingly high proportion of all credit card thefts are from car glove compartments.
- ✓ Know who has access to your cards; don't lend your card to anyone. If a family member (spouse, child, and parent) borrows your card, with or without your acknowledgement, you may be responsible for their purchase/cash withdrawal.
- ✓ Always check your card when you get it back in a store or restaurant. It's easy for you to forget your card when you're in a hurry. It's easy for waiters or sales people to give you the wrong card when they're in a hurry.

- ✓ Carry your cards with you when you travel. When you can't, for instance at the beach, put them in the hotel or motel safe. Never leave your cards in your hotel room, not even in a suitcase.
- ✓ Report a lost or stolen card to the issuing institution immediately. Most fraudulent use of cards takes place within a few days of their being lost or stolen.
- ✓ If your wallet is stolen, be aware that a driver's license and major credit card are often all a thief needs to open charge accounts in your name. To prevent what could be a credit nightmare, ask the credit bureaus (Equifax, 800-525-6285; Trans Union, 800-680-7289; Experian, 888-379-3742) to place a "fraud alert" on your file. After that, any future credit applications will have to be confirmed by you over the phone.
- ✓ Sign the back of a new card as soon as you get it. If you don't a thief could sign it for you and use it.
- ✓ Make a comprehensive list of all your cards and their phone number. Store it in a safe place. (Your wallet is not a safe place). This is key information you'll need to report lost or stolen cards.
- ✓ Only carry the cards you need immediately, in case of theft or loss.
- ✓ If you aren't using your cards, lock them up. Limiting the number of cards you carry limits the potential of fraud.
- ✓ Periodically check your cards to make sure none are missing.
- ✓ Destroy unwanted cards so no one can use them.
- ✓ Never write your card number on a post card or on the outside of an envelope. Also never mail a post card with personal information, such as birth date, social security number, or account number on it. Always place it in a sealed envelope before mailing.
- ✓ When using a telephone credit card in a public place, shield the keypad with your hand or body.
- ✓ Always check your monthly statement.
- ✓ Keep your sales slips and check them off against your monthly statement. To make sure no one else has used your card, or a dishonest merchant didn't alter your sales draft.
- ✓ Report any errors or unknown charges immediately.
- ✓ Destroy your billing statement before you discard it to prevent your account information from falling into the wrong hands.

- ✓ Know when your statement is due and contact your credit union immediately if you don't receive it on time.

Safety when using ATMs

- ✓ Be careful when using freestanding ATM machines, especially at night.
- ✓ Take someone with you, if possible. If the lights in the ATM facility aren't working, don't use the machine.
- ✓ Have your card ready before approaching the machine.
- ✓ Make sure no one can see you punch in your PIN number. Shield the keypad with your body.
- ✓ Don't count your money. Put it in your pocket and walk away. You can count it later.
- ✓ Always take your receipts away with you.
- ✓ At a drive-up ATM, keep all your doors locked and all passenger windows rolled up.

Miscellaneous Safety Tips

- ✓ Be wary if you sign with a company for "credit card registration and protection," to notify all your accounts if your cards are lost or stolen. Read the contract carefully – will you be reimbursed if you notify them properly but they fail to notify your card issuer on time?
- ✓ Notify the post office immediately if you change your address.
- ✓ If you are not receiving mail, call the post office immediately. Some crooks will forge your signature and have your mail forwarded elsewhere, for the purpose of obtaining information that will allow them to apply for credit in your name.
- ✓ If you are told of a forwarding order placed on your mail without your knowledge, go to the post office to check the signature and cancel the order. Ask the post office to track down the forwarded mail – it can remain in the postal system for up to 14 days so it may not yet have landed in the criminal's hands.
- ✓ Call the U.S. Postal Office crime hot line at 800-654-8896 if you are victimized by mail fraud.