

# LET US KNOW IF YOU'RE TRAVELING

As a reminder, if you plan to travel, check to see if your destinations include areas of the United States or foreign countries that have high rates of fraud. Because NavyArmy wants to protect you from becoming a victim of fraud, we limit debit card use in locations that have a high incidence.

We can minimize (or prevent) inconvenience if you let us know your travel plans in advance. For more information, call us at 1-800-622-3631 or visit a branch.

# BLOCKING FRAUDULENT DEBIT CARD ACTIVITY

In our global economy, debit card fraud can take place anywhere in the world! NavyArmy uses blocking tools that allow us to better control debit card fraud by blocking transactions where the incidence of fraud is high.

However, even in blocked countries or within certain merchant categories, members are able to use their NavyArmy debit card by conducting a PIN transaction.

In the event your debit card is denied or for more information, please call or visit one of our offices to request your card be granted temporary access.

## ATM LOCATIONS

NavyArmy provides ATMs at each branch location. To find a NavyArmy ATM near you, visit [navyarmyccu.com](http://navyarmyccu.com).

## SHARED BRANCH NETWORK

As an added convenience, NavyArmy offers members the National Shared Branch Network, which enables you to transact NavyArmy business at hundreds of credit union locations across the U.S. Visit [navyarmyccu.com](http://navyarmyccu.com) to find a shared branch location or ATM in your area.

## IMPORTANT NUMBERS

### To Suspend a Lost or Stolen Card:

Monday-Friday, 8am-5pm 1-800-622-3631  
Weekends or after 5pm CST 1-800-472-3272

### Activate a New Debit Card: 1-800-992-3808

Must call from the phone number listed on your account.

Cards can also be activated by performing a PIN based transaction such as an ATM withdrawal.

### Suspect Fraud:

Call NavyArmy to discuss 1-800-622-3631  
Fraud text alerts come from 20733  
To verify or dispute charges 1-800-279-2674 (English)  
1-877-273-5901 (Spanish)

**NavyArmy**  
COMMUNITY CREDIT UNION

1-800-622-3631  
P.O. Box 81349  
Corpus Christi, TX 78468

[navyarmyccu.com](http://navyarmyccu.com)



**ATM & Debit Card Security**

**NavyArmy**  
COMMUNITY CREDIT UNION

# ATM-DEBIT CARD SAFETY



To offer convenience to members, NavyArmy offers a network of ATMs. When you are using your debit card at any location, to reduce the risk of becoming a victim of fraud, please remember these recommendations:

- Treat your card like cash. Keep it in a safe place.
- Keep your personal identification number (PIN) a secret and block the view of others when entering the PIN.
- Do not disclose card information over the phone to anyone. No one needs to know your PIN, not even your financial institution.
- Never disclose information about your card in response to an unsolicited email, text, or other form of request.
- Make certain your Internet shopping sites are secure, such as checking that a web address begins with "https."
- Report a lost or stolen card at once by calling us at (800) 528-2273.
- Carefully review your account statements for unauthorized transactions.

## SECURITY TIPS WHEN USING ATMS

- Observe the ATM surroundings before approaching a walk-up ATM. If anyone or anything appears suspicious, cancel your transaction and leave the area at once.

- If an ATM is obstructed from view or poorly lighted, go to another ATM. It is a good idea to take along a companion when using an ATM, especially at night.
- Minimize time spent at the ATM by having your card out and ready to use. Do not let anyone see how much money you withdrew, and never count your money at the ATM.
- Never allow a stranger or anyone else to assist you or enter your PIN while conducting an ATM transaction, even if you have trouble or your card is stuck.
- Stand between the ATM and anyone waiting to use the terminal so that others cannot see your PIN or transaction amount. Block the view of others when using a card scanner terminal in a store.
- Look for possible fraudulent devices attached to the ATM. If the ATM looks different or appears to have any alterations or attachments to the card slot or PIN pad, do not use it. If you are prompted to enter your PIN twice, or if you notice unusual messages on the screen, go to another ATM.
- If using a drive up ATM, keep the doors locked, windows up and engine running when waiting in line. Leave enough room between cars to allow for a quick exit if necessary.
- If anyone follows you after you have completed your ATM transaction, go immediately to a crowded, well-lit area and call the police.
- Be sure the transaction is complete and you have received a receipt before leaving. If you received cash back, put it away before leaving the terminal.

## TIPS FOR ONLINE AWARENESS

Phishing email messages, designed to get you to reveal personal information, are more sophisticated than ever. We want you to be aware of things to look for before you consider answering or clicking on a link in an email. If a message you receive, even supposedly from someone you know, has misspelled words and strange language or links and attachments, look at it carefully. Be suspicious and don't click on anything or download an attachment until you confirm it is a valid email from the sender.

### BASIC TIPS TO REMEMBER:

- Be suspicious of unexpected messages directing you to click on a link or to open an attachment
- Your Web browser is your primary tool for using the Internet, so keep it updated with the latest security patches from the vendor
- Antivirus software is an important tool to safeguard your computer, so make sure it is always enabled and contains the latest virus updates from the manufacturer
- Don't trust a site just because it claims to be secure, make sure you are purchasing merchandise from a reputable source

