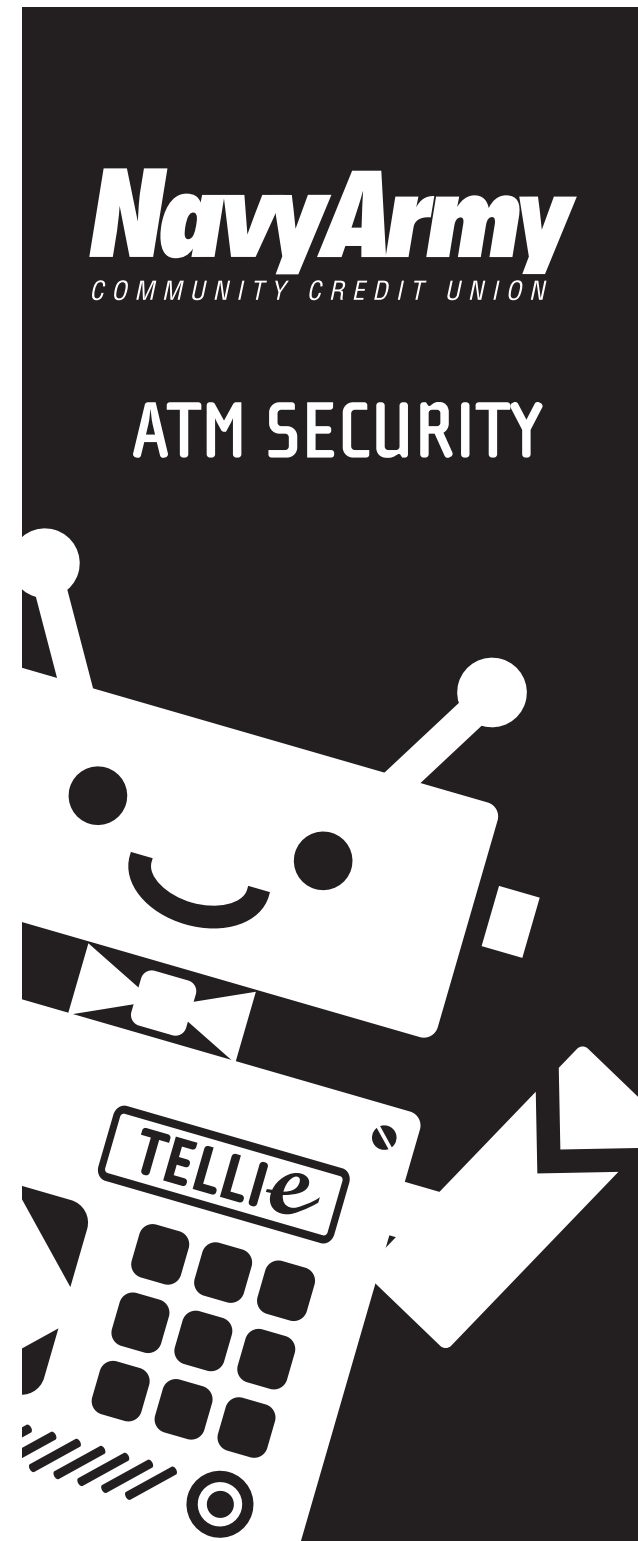## ATM-Debit Card Safety

To offer convenience to members, NavyArmy offers a network of ATMs. When you are using your debit or ATM 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 number.

• 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.

NavyArmy
COMMUNITY CREDIT UNION

ATM SECURITY

TELLIe

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 (361)986-4500 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.

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 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

ATM LOCATIONS
Corpus Christi ATM's

- Airline - 522 Airline*
- Navy Exchange - NAS Corpus Christi - Bldg. 1744
- Spohn Branch - 5725 Spohn Drive*
- NAS Corpus Christi Branch - Building 125
- CCAD Building 8, NAS - Corpus Christi
- Flour Bluff Branch - 9552 S.P.I.D.*
- Flour Bluff Branch - 9552 S.P.I.D.* (lobby)
- Northwest Branch - 12129 Leopard*
- Crosstown Branch - 4802 Crosstown Expressway*
- Crosstown Branch - 4802 Crosstown Expressway* (lobby)

Surrounding Area ATM's

- Portland Branch - 285 Buddy Ganem*
- Kingsville - 2940 South Brahma*
- Beeville Branch - 2505 N. St. Mary's*
- Beeville Branch - 2505 N. St. Mary's* (lobby)

Rio Grande Valley ATM's

- Brownsville Branch - 2100 FM 802 Ste.2055*
- McAllen Branch - 4015 North 10th Street*

* ATM accepts deposits.