ATM Safety Tips

Protect yourself when using an ATM.

General ATM, debit and credit card security.

- Always sign your card(s) on the signature panel.
- Protect your cards as if they were cash. Do not leave them unattended anywhere. Keep your cards in a safe place and never leave them or personal identity documents lying around at home, at work, in a vehicle or in public places.
- Do not let your bag or wallet containing your cards out of your sight in public places.
- Make a list of your card account numbers and telephone numbers for reporting lost or stolen cards. Keep the list in a safe place. Check your cards periodically to make sure none are missing.
- Check your credit report annually.
- Cut up expired or old cards.
- Shred old credit card statements, account statements and related information that you no longer need.
- Never give your credit card number over the phone or Internet unless you are dealing with a reputable company or you have personally initiated the call.
- Remember, we will not call you to verify your account information including any of your account or card numbers or PINs.

Set up card alert.

- To set up an alert on your Debit Card to notify you when a debit card transaction is in process on your account, log in to www.members1st.org> Members 1st Online> checking account> click on “alert me” in the upper right corner.

- To set up an alert on your VISA Credit Card, log in to www.members1st.org> Members 1st Online> click on your VISA Credit Card account> click alerts on the left side of the screen.

- To set up a travel notice for your Debit and/or VISA Credit Card, log in to www.members1st.org> Members 1st Online> Services> Card Services> Travel Notices.

If you have a Debit, Credit or ATM card that has been lost, stolen, damaged, or have identified known or suspected fraud, please call us:

**VISA Debit & ATM Cards**
(800) 826-4314
(414) 341-4015 (if calling from overseas)

**VISA Credit Cards**
(800) 826-4314
(800) 847-2911 (if calling from overseas)

**Identity Theft & Other Fraud**
(800) 826-4314

Report Suspicious Emails, Phone Calls or Text Messages:
If you receive a suspicious e-mail, phone call or text representing itself as Members 1st Federal Credit Union, please notify us by either:

- Sending the information to: scam@members1st.org; or
- Calling (800) 826-4314

5000 Louise Drive
P.O. Box 40
Mechanicsburg, PA 17055
members1st.org

Federally insured by NCUA
Choose your ATM carefully.
- Use ATMs that are familiar when possible. If that’s not possible, choose well-lit, well-placed ATMs where you do feel comfortable. Avoid secluded or hidden ATMs. Scan the entire ATM area before you approach it. Avoid using the ATM altogether if there are any suspicious-looking individuals around or if it looks too isolated or unsafe.
- Always have your card ready in your hand before you approach the ATM. Avoid opening your purse, bag or wallet while in the queue for the ATM. Carry your cell phone with you in the event a situation arises.
- Check for unusual instructions on the display screen and for suspicious blank screens. If you suspect that the ATM has been interfered with, proceed to another ATM.
- Avoid ATMs which have messages or signs fixed to them indicating that the screen directions have been changed, especially if the message is posted over the card reader. Financial institutions and other ATM owners will not put up messages directing you to specific ATMs nor would they direct you to use an ATM that has been altered.
- If the ATM looks significantly unlike any you’ve ever used or the machine appears to have attachments on the card slot or number pad, do not use it. If the machine offers unfamiliar options, don’t use it. Report anything suspicious about the machine to the financial institution that owns the machine.
- If you are followed after using an ATM, go to a heavily populated, well-lighted area and call the police.

Follow directions.
- Follow the ATM instructions carefully, especially if you’re using a particular machine for the first time.
- If an ATM keeps your card, do not re-enter your PIN. Notify us immediately.
- If the ATM instructions ask you to re-insert your card in a second card reader at the machine, do not do it. Notify us immediately.
- If you become suspicious for any reason while using an ATM, hit “cancel” and leave.
- Don’t keep your Personal Identification Number (PIN) with your ATM card or write it on your card.

Monitor your ATM transactions.
- Keep all receipts from ATM transactions to help you keep track of exactly when and where you’ve used your card.
- Always know how much money you have available in your account. Examine your statements to identify unauthorized transactions. Report any suspicious transactions immediately.
- Do not be in a hurry during the transaction, and carefully secure your card & cash in your wallet, handbag or pocket before leaving the ATM.

Using indoor or walk-up ATMs.
- Avoid letting anyone who you do not know come in with you or stand too close to the ATM. If necessary, pretend you forgot something and leave.
- Stand directly in front of the ATM to ensure transaction privacy. Shield the screen and keypad with your body as you use an ATM to prevent others from seeing your Personal Identification Number (PIN).
- As soon as you are finished with your transaction, take your cash, card, receipt and leave. Don’t stand at the machine and count your cash or take time putting it into your wallet. Avoid counting your money at the ATM or in public. Count your cash in your car with your car doors locked.
- Don’t leave your car unlocked and unattended with the engine running. Your car can easily be carjacked while you’re busy conducting your transaction.

Using drive-up ATMs.
- Keep your car running and your car doors locked. Make sure your passenger windows are rolled up.
- While waiting in the car line, leave enough space between you and the car in front of you so that you are able to maneuver your car for a quick get-a-way if you need to drive away.

Secure your card and account information.
- Never force your card into the card slot.
- Memorize your PIN. Never disclose your PIN to anyone. Do not use obvious and guessable numbers for your PIN like your date of birth, address, last four digits of your Social Security Number and the like.
- Change your PIN periodically and if you think it may have been compromised, change it immediately.
- If your card becomes stuck in the ATM or you experience difficulty with your transaction, don’t accept help from anyone. Do not allow anyone to distract you while you are at the ATM.
- If your card gets jammed, retained or lost, or you experience any kind of interference at an ATM, call us immediately.
- Press “cancel” and withdraw your card and proceed to another ATM if the machine is not working properly. Alert us of any technical problems you experience.
- Follow the instructions on the display screen. Do not key in your PIN until the ATM requests you to do so.
- Regularly check your account balance and account statements and alert us of any discrepancies.

Point of Sale precautions.
Be alert as to what is happening with your card when performing a transaction. For example, do not let a restaurant server take your card away to settle the account. Watch while cashiers process your card and make sure they do not insert it into or swipe two different devices. Always check your receipt.