

Debit Card Safety Tips and Precautions

Using your debit card is a simple, hassle-free way to get cash, make purchases, and much more. Unfortunately, in this day and age, the potential for fraudulent debit card transactions has become a concern both for card users and financial institutions. From time to time, we may be calling you to ask about the validity of a debit card transaction. Your debit card transactions are monitored for potentially fraudulent activity which may include sudden changes in location. **If you are going to use your card outside of the United States or are taking a vacation out of state, please give us a call and let us know when you are leaving, when you will return and where you are going.** If we do call you, your participation in responding to our call is critical to prevent potential risk and avoid restrictions we may place on your card. To ensure we can continue to reach you whenever potential fraud is detected, please keep us informed of your correct phone number, mobile number, e-mail and mailing address at all times.

If we call you, the staff person will identify themselves and ask to verify recent transaction activity on your card. We **WILL NOT ASK** for your card number, the CVV code on the back of your card, your account number or social security number. We're here to help protect your account. You can help by carefully monitoring transaction activity on your account and by contacting us *immediately* at **860-292-2940** if you identify any fraudulent transactions or if your card is lost or stolen.

Here are a few key items to keep in mind when using your card:

1. Unless absolutely required for a legitimate business purpose that you initiate, avoid giving out your address, phone number, date of birth, social security number, card or account number and your card's expiration date.
2. Your PIN is private, NEVER give it out or lend your card to anyone.
3. When using your card, cover it and your PIN and be on the lookout for anyone watching your transaction or cashiers taking your card out of sight. Also, if you feel uncomfortable at one particular ATM, go to another.
4. You should never respond to unsolicited emails that ask you to verify your card or account number or provide a link to any website. Such sites can look legitimate but may collect your personal data or install spyware on your computer.
5. Keep your computer's virus protection up to date. Use spyware and malware detection. Update your computer frequently with recommended security patches.