Debit Card Safety

Debit card fraud is a common form of identity fraud that can affect anyone. It is important to protect your debit card as well as your account number, expiration date, security code (the three-digit number on the back of your card), and your PIN. Identity theft can occur even if you don't lose or misplace your debit card. Someone who has learned your account number, security code, and PIN can use that information to access your account, withdraw funds, or create counterfeit cards. While in many cases you are not responsible for unauthorized transactions, it can be a hassle to resolve the situation.

Tips to Avoid The Risk of Debit Card Fraud:

- Never write your PIN on or near your card. Memorize it instead.
- Don't give out bank account information over the phone or the Internet unless you have initiated the contact or you know the person is who they claim to be. Beware of deceptive calls or emails from individuals claiming to be from your bank asking you to "verify" your account information. A true bank representative would **never** ask for your PIN because your bank already has that information.
- Don't share your PIN, security code or other account information with friends or relatives who aren't co-owners of your account. Never reveal this information to new friends you meet over the Internet. Common scams occur with a false job offer or Internet friendship or romance, in which the victim is asked to transfer money to the perpetrator.
- Take precautions at the checkout counter, ATM, and gas pump. Always stand so that no one can see the keypad where you enter your PIN. At retail establishments, it's best to use do-it-yourself scanners. If you give your card to a clerk, make sure they don't run your card through two scanners instead of one. The second scanner could be capturing your account information to make a counterfeit card. In general, be alert for suspicious-looking devices that may be used to "skim" information from your card.
- If you use your debit card to shop online, consider extra precautions with your personal computer. Use similar precautions with Internet and mobile banking. Experts advise installing virus and spyware protection to stop thieves from secretly installing malicious software that can be used to spy on your computer and obtain account information.
- Look at your bank statements as soon as they arrive. Or better yet, review your account each week. Promptly report any discrepancy, such as a missing payment or an unauthorized transaction, to your bank. Your quick attention to the problem may help limit your liability and give law enforcement authorities a head start on stopping the thief.