



## WE MAY BE CALLING YOU!

To protect your account, we monitor your ATM and Debit Card transactions for potentially fraudulent activity which may include a sudden change in transactions taking place in the foreign country, a sudden string of costly purchases, or any pattern associated with new fraud trends that Metro North FCU has been made aware of.

Before traveling outside the U.S. be sure to contact us to find out if your card will work in the country you plan to visit or if you need to make arrangements with MNFCU to have your card unblocked while you are away. Foreign countries have a higher volume of fraudulent activity and for your protection we have blocked countries we know to have a high crime rate of fraudulent activity.

If we suspect fraudulent ATM or Debit card use, *we'll be calling you* to validate the legitimacy of your transactions. Your participation in responding to our call is critical to prevent potential risk and avoid restrictions we may place on the use of your card.

- ⇒ Our automated call will ask you to verify recent transaction activity on your card.
- ⇒ You'll be able to respond via your touchtone keypad.
- ⇒ You'll also be provided with a toll-free number to call should you have additional questions.

Our goal, quite simply, is to minimize your exposure to risk and the impact of any fraud. To ensure we can continue to reach you whenever potential fraud is detected, please keep us informed of your correct phone number and address at all times.

In the meantime, please be diligent in monitoring transaction activity on your account and contact us immediately if you identify any fraudulent transactions. Here are some additional tips on protecting yourself from Debit card fraud:

1. Unless absolutely required for a legitimate business purpose, avoid giving out your:
  - ⇒ Address and ZIP code
  - ⇒ Phone number
  - ⇒ Date of birth
  - ⇒ Social Security number
  - ⇒ Card or account number
  - ⇒ Card expiration date

*Your PIN is private; never give it out.*

2. In stores and at ATMs, always cover your card and PIN, and watch for:
  - ⇒ Cell phone cameras, mirrors, or other tools used to view cards and PINs
  - ⇒ People watching your transactions
  - ⇒ Cashiers taking your card out of sight; take it to the register yourself
  - ⇒ Any unusual activity at ATMs; if you feel uncomfortable, go to another ATM
3. Online, you should never respond to unsolicited emails that:
  - ⇒ Ask you to verify your card or account number; such emails are not sent by legitimate businesses
  - ⇒ Link to websites; such sites can look legitimate but may collect data or put spyware on your computer