We May Be Texting, Emailing or Calling You

To protect your account, NBT's Fraud Center monitors your ATM and debit card transactions for potentially fraudulent activity which may include a sudden change in locale (such as when a U.S. issued card is used unexpectedly overseas), a sudden string of costly purchases, or any pattern associated with new fraud trends around the world.

If we suspect fraudulent ATM or debit card use, the NBT Fraud Center will text, email and call you in order to validate the legitimacy of your transactions. Your participation in responding to our communication is critical to prevent potential risk and avoid restrictions we may place on the use of your card.

- Our automated communication will ask you to verify recent transaction activity on your card.
- You will be able to respond via text, email or your touchtone keypad.
- You will also be provided 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. Some additional tips on protecting yourself from debit card fraud are provided as follows:

- 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

- In stores and at ATMs, always cover your card and PIN (Personal Identification Number), 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

- 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

Your PIN is private, NEVER give it out.