



**GULF COAST BANK**  
& Trust Company

## **WE MAY BE CALLING or TEXTING YOU**

To protect your account, we monitor your ATM and debit card transactions for potentially fraudulent activity which may include but are not limited to 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, *we'll be calling or texting\* you* to validate the legitimacy of your transactions. Your participation in responding to our call or text is critical to preventing potential risk and avoid restrictions we may place on the use of your card.

You must Opt In for Two Way Texting. If you have not, you will receive a call.

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

If you have Opted In for Two Way Texting, you will receive a text from us.

- A text message will ask if you are attempting to use your debit card at a particular merchant and for a specified dollar amount.
- You'll be asked to respond "YES" or "NO".
- If you respond "YES" you will be able to continue to use your debit card.
- If you respond "NO", a temporary hold may be placed on the debit card and you will be asked to call.

\*Message and data rates may apply. Please check with your service provider for specific fees and service charges.

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. If you need to update your contact information, please contact your local branch or call Customer Service at 1-800-223-2060.

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:

### **Protect yourself**

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.*

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

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