Capital Bank™

# Protect yourself against fraud

The security of our customers is a priority for Capital Bank.
We believe the more you know, the better prepared you will be to recognize and prevent fraudulent activity.

- **NEVER** provide personal information to unsolicited calls or text messages.
    - This includes: your full Social Security number, driver's license number, account numbers, personal identification numbers (PINs) or your 3-digit card verification codes.
- Do not always trust caller ID – it can be faked.
- If you feel a call or text message may not be authentic, hang up and call back to a number you know is correct.
- Diligence and account monitoring is the first line of defense when it comes to stopping fraud.

## Important Card Information – Capital Bank Fraud Alerts

**Two-Way Text Alerts** – A text alert from us will always be from a 5-digit number. A valid notification will provide information about the suspect transaction and ask the cardholder to reply to the text message with answers such as "yes", "no", or "stop". We will never ask you to click a link.

**Fraud Department Telephone Alerts** – A phone call from our institutions automated dialer will only include a request for your zip code, and no other personal information, unless you confirm that a transaction is fraudulent. Only then will you be transferred to an agent who will ask questions to confirm that you are the actual cardholder before reviewing your transactions.

If a voice call is received from our Call Center asking to verify transactions, no information will be requested other than the cardholder's zip code, and a "yes" or "no" to the transaction provided.

If at any point you are uncertain about questions being asked or the call itself, hang up and call us directly at (713) 675-2341 or for after-hours service, selection Option 2.

We will NEVER ask you for your PIN, the 3 digit security code on the back of your card, debit card number or social security number.