FRAUD PROTECTION

Fraudsters have become increasingly skillful at getting cardholders to share the information they need to commit fraud.

Below are points to remember:

- We will never call you to request information you received via text (SMS) or pressure you to reset you online banking password.
- A text alert from us warning of suspicious activity on your account or card will **NEVER** include a link to be clicked. Never click on a link in a text message that is supposedly from us. A text alert from us will always be from a 5-digit number and **NOT** a 10 digit number resembling a phone number.
- Use caution when making online purchases. If it sounds too good to be true, it has a high probability of fraud.
- When being solicited for charitable donations over the phone, don't give your card information directly to the solicitor. Use the charitable organization's website instead.
- Don't trust caller ID: Caller ID may be modified to show your financial institution's name.
- Don't provide your online banking log in credentials, password, debit card number/code, account number or personal information by email, text or on an unsolicited call. Contact your local United Bank & Trust branch directly or call us at 785-562-4312.
- We will NEVER call and ask you for your Debit Card PIN, 3-digit security code on the back of your card. Don't give this out to an unsolicited caller, no matter what they say. Hang up and call us directly.
- Don't click on links in unsolicited emails or texts.
- Don't give an unsolicited caller remote access to your computer.

MONITOR YOUR ONLINE ACCOUNT

To help detect fraud quickly, we recommend checking your online banking account regularly. Consider enrolling alerts to receive notifications of account activity. If anything looks amiss, call us directly for assistance.