UNITED BANK together with Zelle®

1. Only Send Money To People You Trust

Zelle® should only be used to send money to, or receive money from people you trust. If you are unsure of a recipient's email address or U.S. mobile number, you should contact the recipient to confirm their information before using *Zelle* to send them money. Neither *Zelle* nor United Bank offer a protection program for any authorized payments made with *Zelle*. With these parameters, it's safest to only use *Zelle* with confirmed friends, family, co-workers and members of your community that you trust.

2. Use Unique Credentials

To protect your bank account, it is vital to use a unique password within the *Bank With United* app. Use a password you have never used for another account and will not use for one in the future. It is easier to repeat one password across all applications, but that heightens your vulnerability. The *Bank With United* mobile banking service utilizes best practices from online banking, such as HTTPS, 128-bit SSL encryption, or password access and application time-out when your mobile device is not in use. Only the mobile devices that you personally enroll in the service can access your accounts. In addition, no account data is ever stored on your mobile device.

3. Monitor Bank Activity

Regularly keeping track of your bank account activity will make sure you can quickly investigate any issues. We regularly monitor activity in our app and will alert you of any potential fraud or suspicious activity related to your bank account. We have security algorithms analyzing your account trends so when an unordinary transaction comes across the system, we will alert you and verify that the transaction was legitimate or if it were fraud. However, the most effective way to protect yourself is regularly monitoring your activity.

4. Protect Your Account

If your phone has been lost or stolen, or if you notice suspicious activity on your phone, please immediately contact our Customer Service Center at 1.800.327.9862. In order to protect your accounts, we can subsequently disable *Zelle* on your mobile banking profile and temporarily remove access to your mobile and online banking features. You have the ability to temporarily or permanently disable your account at any time by calling us at 1.800.327.9862.

5. SIM Card

Only specific cell phone carriers use SIM Cards, but if you use a SIM Card with your mobile device, we strongly suggest that you contact your cell phone carrier and make sure your personal information is accurate and secure. There have been reports across the telecommunications industry that fraudsters have found vulnerabilities with how companies verify information when replacing a customer's SIM Card. Most cell phone carriers allow their customers to add additional security to protect their account, like using an account PIN.

6. Responsible Online Practices

We recommend that our online and mobile banking customers routinely review the security of their personal information across all online services that they currently use. Recommended online practices include putting a passcode lock on your mobile phone, never sharing your personal information via email or text, and being aware that fraudsters have the ability to pose as legitimate companies. United Bank will never ask you to share your personal information over text or email.