STAY SAFE USING PEER-TO-PEER PAYMENT APPS

FirstBank

Mobile Payment Apps, (also known as P2P Apps), such as Zelle, Venmo, PayPal, & Cash App have become increasingly popular when exchanging money with friends and family. Despite the growing popularity, consumers should be aware that these payment apps are just like cash. Once you send the money, it's gone. You should never pay someone using one of these apps unless you specifically know the person. The best method of fraud and scammer protection is to never use the apps as a means to pay for goods and services to someone you do not know.

Consumers have limited protection from fraudulent and unauthorized activity from these apps.

AVOID SENDING MONEY TO A SCAMMER

Don't click on links in an unexpected email, text message, or direct message that asks you to send money. Don't give out your username, PIN or password.

Verify that you know the person you are sending money to.

Double-check all information to make sure it's correct before sending money to those you know.

FIRSTBANK DOES NOT ASK FOR:

- One-time passcodes
- Passwords of any kind
- Full Social Security number
- PIN number
- Debit or credit card 3-digit security code or expiration date
- Online banking secret word or password
- Account number

As your bank, we already know this information. If anything sounds unusual, trust your gut! Hang up and contact us using a trusted channel!

PROTECT YOUR ACCOUNTS

- Use multi-factor authentication
- Set up alerts in your app
- Check your payment app and bank accounts regularly
- Never share your credentials

Paid a Scammer Through a Payment App?

- Report it to the payment app or service and ask to reverse the transfer
- Contact your Financial Institution
- Report it to the Federal Trade Commission at reportfraud.ftc.gov

 P2P-022022