Digital Payment Scams Information

Digital payment platforms are becoming a more popular, quick, and convenient way to send money. As the use of P2P apps, such as Venmo, Cash App, and Zelle, continues to rise, unfortunately, so do the scams. Fraudsters are becoming tricker with their scam tactics in order to fool victim's into giving up their cash – especially with P2P transactions being instantaneous and usually hard to reverse. It is important for our customers to be educated and aware of these scams to avoid becoming a victim.

Here is how the latest type of scam works: *

- It starts with fraudsters sending account alerts to Customers via text message – appearing to come from the Bank – asking if they attempted a large dollar Zelle transfer. The user is given the option to choose "YES" or "NO".
- If the user responds "NO", the fraudster will call the Customer spoofing the Bank's phone number, claiming to be from the Bank's fraud department.
- Fraudster tells the user their Zelle transfers can be recoverable.
- Fraudster then tells the user that in order to recover the stolen funds, user must use Zelle to transfer the funds to themselves using the users' mobile phone number. However, first, the user needs to disable their phone number associated with their Zelle account. When the fraudster links the user's mobile phone number to the fraudster's Zelle account, a 2-factor authentication passcode is generated and sent to validate the mobile phone number. The text message containing the passcode is actually sent to the user's mobile phone; however, the fraudster cons the user into providing the passcode over the phone.
- Fraudster enters the passcode to activate the mobile number on their Zelle account, and user is instructed to Zelle themselves the funds.
- The Zelle transfers instead go to the fraudsters.

There have been other cases where the Customers refused to provide the passcode to the fraudsters, the fraudsters impersonated the Customers and social engineered the Customers' mobile phone carrier and were successful in porting the Customers' mobile phones to a different carrier. Other Banks reported that fraudsters successfully social engineered the Bank's call center employees into changing mobile phone numbers on Customer accounts allowing the fraudsters to receive the passcodes. In some cases, the fraudsters hacked Customer email accounts to intercept passcodes sent via email. These tactics allowed fraudsters to intercept the passcodes needed to login to Customer accounts.

For years, scammers have been making up all kinds of stories to trick people into sending them money*. Other ways scammers lure people in are by saying:

- You won a prize or a sweepstakes and need to pay some fees to collect it.
- A loved one is in trouble, and they need you to send money.
- You owe taxes to the IRS.
- They're from tech support and need money to fix a problem with your computer.

Digital Payment Scams Information

- They're romantically interested in you and need your money.

If you get an unexpected email or text message that asks you to send money, **don't click on any links**. If you sent money to a scammer, report the scam to the mobile payment app and ask them to reverse the transaction right away. Then, report it to the Federal Trade Commission. When you report a scam, the FTC can use the information to build cases against scammers.

*Mobile Payment Apps: How to Avoid a Scam When You Use One, Federal Trade Commission;

Remember if you have any questions on whether the bank or IRS is calling you, hang up and call back on the normal publicly published phone number.