Avoid Fraud on Money Transfer Apps

Mar 21, 2022

Don’t Become a Victim of Fraud When Using Money Transfer Apps

Consumers need to be extremely cautious when using money transfer apps such as Zelle, Venmo, or Cash App because these apps transfer funds instantly, which makes them preferred payment methods for scammers. A recent New York Times article described elaborate schemes fraudsters are using to trick consumers into sending them funds on Zelle, the country’s most widely used money transfer service.

Several of America’s largest banks collaborated on developing this app in 2017 to enable instant, digital money transfers and embedded it in their systems. Today, the Times reports, 1,425 banks and credit unions offer Zelle through digital or mobile access for money transfers. It’s popular with the public because it’s quick, easy to use, and free of charge. One safeguard with Zelle is that banks can customize the app by placing limits on transaction amounts and may add their own security settings. At Maspeth Federal Savings, personal account holders may use Zelle to transfer funds to a company or an individual up to $500 per day. (Click here for further information.)

Since banks of all sizes consider payments through these transfer apps to be irreversible, says the Times, it’s advisable to verify the identity of everyone requesting payment through a money transfer app. Some scammers are impersonating bankers with caller ID’s that makes it look as if a call is from a bank or with spoofed bank email addresses.

These guidelines may help you prevent yourself from being tricked into sending funds to fraudsters:

- **Never send funds to yourself through a money transfer app.** If a caller (who’s impersonating a bank official) tells you that fraud has occurred on your account and the only way to get the money back is to send funds to yourself, don’t do it. This is a technique that scammers use to get your personal information and steal your funds, according to an FBI official who spoke to an ABC affiliate in Chicago. Although your name is in the “to” and “from” sections, scammers have been able to divert funds when you hit “send” to another bank.

- **Never read back verification codes to someone requesting them.** A phone call requesting these codes should alert you that the person you’re dealing with is a scammer.

- **Beware of fake Zelle emails.** Zelle will never email you or call you to request money. Fraudsters may try to trick you into clicking on a phishing email. Look out for emails with poor grammar or spelling errors and hover over a sender’s email address to make sure it’s not phony.

- **Do not provide confidential account information to unidentified individuals.** Legitimate companies would not ask a customer to transfer funds between accounts nor request sensitive account information such as an account number, Social Security number, or Tax ID over a text, an email, or a digital message.

- **Do not send funds in response to phone calls or text messages you weren't expecting.** Remember that Caller ID and phone calls from numbers you recognize could be spoofed to appear to be from legitimate callers. Verify a caller or emailer's identity through a company's website if possible. Don't send funds to anyone whose identity you cannot verify.

- **Use money transfer apps only to send funds to people and companies you know.** Keep in mind that sending funds via a money transfer app is like sending cash.

- **Use multi-factor authentication and PIN numbers on apps that offer them.** Each layer of security that's offered helps prevent fraud.

The bottom line is that you must be extremely cautious when using money transfer apps. Do not click on links, open attachments, or sign on to your account from a link in an email or text message that appears to come from your bank. Instead, delete the message and contact the bank.