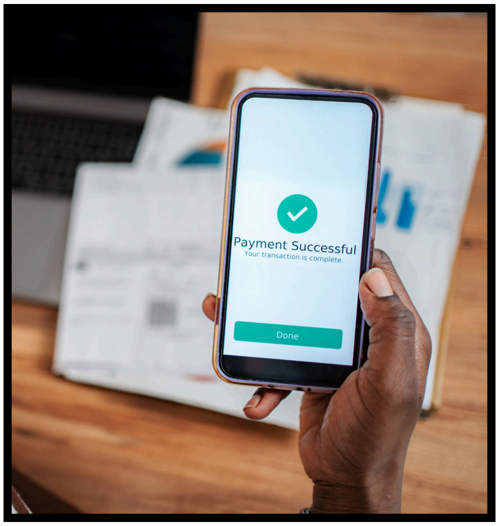
SCAM ALERT: PAYMENT APP FRAUD



WHAT ARE PAYMENT APPS?

Mobile payment apps are a convenient way to send, receive, and manage money using your smartphone. Most mobile payment apps connect to your bank account, debit card, or credit card, making it easy to transfer money, pay bills, shop online, or make purchases in stores.

Some popular payments apps are Venmo, Cash App, Zelle, and PayPal.

HOW DO SCAMMERS USE PAYMENT APPS TO STEAL MONEY OR PERSONAL INFORMATION?

Scam 1: Accidental Payment Scam

A stranger may send you a payment, then contact you to say they sent it by mistake. They will then ask you to send the money back as a new payment. Cyber-criminals are using stolen credit card information to act like they are sending you money. Once the card is reported as stolen, the credit card company will refund the fraudulent transfer. Meanwhile, the money you send back to the fraudster comes directly from your account!

What to do if this happens to you:

- **NEVER** exchange payments with people you don't know.
- If you don't know the person who paid you, contact customer support so they can help reverse the payment.
- To help prevent this from happening in the future, block the users who send unsolicited payments or requests.
- **NEVER** communicate with the person who sent the money! They will give you a sad story of what will happen if you don't send the money back.
- If someone truly sends money by accident, they need to contact the app to have the transaction reversed as soon as possible.

ALABAMA SECURITIES COMMISSION
1-800-222-1253
ASC.ALABAMA.GOV

Scam 2: Fraudulent Activity Alert Call or Text from Payment Apps

Scammers may impersonate customer representatives from payment apps to trick you into giving them account information. They may call or text you to inform you that an unauthorized transaction occurred or that hackers are trying to access your account. They may tell you that they need to secure the account and will need to reset your password.

What to do if this happens to you:

- **NEVER** provide the verification code sent to your phone to anyone.
- **NEVER** tell anyone your password.
- **NEVER** give access to your device remotely.
- **NEVER** install a third-party app.
- **NEVER** allow someone to create another account on your behalf.
- Payment apps will **NEVER** direct you to send money from your account to another user via a different payment platform.
- Payment apps will **NEVER** ask you to send money to "verify" your account.

Scam 3: Imposter Scams

Bad actors may attempt to replicate a profile picture on a fake account to impersonate your friend, co-worker, potential new employer, landlord, or love interest. They will impersonate someone in your social circle and request money.

What to do if this happens to you:

- Reach out to the real person outside of the payment app to verify that the request is legitimate. Pick up the phone and call them on the number you have. The cyber-criminal may provide you with a “new” number, but don’t fall for it.
- If you don’t know the person, **NEVER** give money to someone who you have never met in person.
- Check the creation date and transaction history of the account. If it is a brand-new account with no transaction history, it might be a scam.