View as Webpage

Money Sharing with Peer-to-Peer Apps: What Are the Risks?

Many of us have used peer-to-peer (P2P) payment apps to split a bill, send money to a friend or even use them for traditional shopping. Oak Bank partners with Zelle®, available from online and mobile banking, for clients to send and receive money from friends, family, and trusted people. Peer-to-peer payment apps such as Cash App, PayPal and Venmo are easy to use and convenient, but as their popularity has increased, so have incidents of fraud.

What Are Peer-to-Peer (P2P) Apps?

Peer-to-peer apps, also called payment apps, make sharing money with others simple and convenient by linking to your bank account or card. Users can easily send and receive money through the apps, making things like splitting checks or the cost of a gift a breeze.

There are two types of P2P apps - those offered through banks (ex: Zelle®) and those that are nonbanks (ex: Venmo, Apple Pay, Cash App).

How do P2P Payment Scams Work?

There are lots of ways using a P2P payment system can put you at risk, but the following two vulnerabilities are most common.

1.) The bogus buyer

In most cash-transfer apps, when you receive a payment, the money goes into your P2P system balance and stays there until you transfer it to an external account or use it to pay for another transaction. This transfer usually takes one to three business days to clear. Crooked scammers are taking advantage of that “float” in the transfer process to con you out of your money.

Here's how it works:
A scammer will contact you about an item you’ve put up for sale or tickets to an event. Together, you’ll arrange for an exchange of funds and goods. You may even take precautions against a possible scam by insisting on an in-person meeting for the exchange or refusing to send out the item until you see the money in your P2P account. Things proceed according to plan. You’re notified that the money has been sent to your account and you hand over your item. Sadly, you won’t realize you’ve been ripped off until a few days later when the money transfer does not clear and the contact has disappeared with your goods. Unfortunately, there’s no way you can get your money back, because most P2P providers will not offer compensation for a fraudulent sale. Similarly, your linked financial institution bears no responsibility for the scam and can’t help you recoup the loss.

2.) Publicized payments

PayPal’s Venmo is the only P2P app with a built-in social networking component. This feature has led to a host of privacy issues that have been brought to the attention of the Federal Trade Commission (FTC).

In short, every Venmo transaction you make is up for public scrutiny. No one can access the payment amounts, but anyone who is interested can track the restaurants where you like to eat, the clothing stores you most frequent and check out when you last filled your gas tank. Creepiness factor aside, all that information going public makes Venmo users super-vulnerable to scammers and identity thieves.

Venmo allows you to tweak your privacy settings to keep your information from going public, but most people are unaware of the issue and/or neglect to take this measure. Recently, the FTC ruled that Venmo must make this detail clearer to users. Venmo has since created a popup tutorial for all new users demonstrating how to adjust your privacy settings to keep your transactions from going public. If you choose to use Venmo, check your settings to be sure your money habits aren’t being broadcast for the world to see.

How Can You Protect Your Funds?

- Use bank-supported P2P applications like Zelle® that only sends and receives funds from FDIC-protected bank accounts.
- Only send money to people you know and trust.
- Never use a P2P service for business-related transactions.
- When using Venmo, adjust your privacy settings and opt-out of public tracking.
- Carefully read the terms and conditions of a P2P service before using.
- Accept any security updates offered by the P2P app you use.
- Always choose two-factor identification and use a PIN when possible. If your app and phone allows, choose fingerprint recognition and/or touch ID for added protection.
- Check your recipient's information carefully before completing a money transfer.
- Choose to be notified about every transaction.
- Link an external account instead of keeping your funds in the P2P account.

For additional security information, you can visit Oak Bank's Security Information on our website.

Oak Bank will never ask for personal information over an unsolicited phone call, text, email, or online chat. Never share your account information, PIN number, username/password or one-time password.

If you receive an unsolicited phone call or text message requesting your Oak Bank account information, report it immediately by calling 608.441.6000 or sending an email to bank@oak.bank.

Need help with your account?

Email: bank@oak.bank
Call: 608.441.6000

If your Oak Bank Debit/ATM Card has been misplaced, call 877.755.2957..

If you have misplaced your Oak Bank Visa Credit Card, call 800.423.7503.

Visit Oak Bank Online

608.441.6000
877.625.2265 Toll Free

Lobby
M - F: 8 a.m. - 5 p.m.

Drive-up
M - F: 8 a.m. - 5 p.m.

Member FDIC

STAY CONNECTED

This Oak Bank message may contain promotional content.