FINANCIAL FRAUD consortium

Industry Insight

Peer-to-Peer Scams Impacting Business and How To Recognize It

With the rise in popularity of peer-to-peer payment apps such as Venmo, CashApp, and Zelle, scammers have found new ways to prey on and steal from people in all walks of life: the elderly, the overly compassionate, and even the under-trained employee.

In this blog post, we share more about these scams and how you can protect yourself, your family, and even your employees from falling for these types of scams.

What are P2P Scams?

Today's technology makes it easy to send and receive funds online, but it's also unfortunately true that scammers have found a way to get our hard-earned money through various platforms. While most P2P apps are still safe to use, some aren't as safe as they used to be. Businesses are even beginning to use these apps to accept transactions from their customers, opening themselves up to new vulnerabilities if not appropriately accounted for.

Much like with any other payment method, you will need to handle your business or personal information and money with care. These apps were designed to allow users to issue payments to friends and to people they know, but strangers may also take advantage of these platforms. It can be easier than you think to get caught up in a PayPal scam or Venmo scam.

Things To Look Out for

If you or your employees frequently make or accept transactions through PayPal or Venmo, you may be at risk for payment app scams. Look out for these common scenarios:

- Scammers will claim to be from the fraud department to ask you to confirm sensitive information, such as your bank account information. Other details they might ask for are data such as debit or credit card numbers, or even your Social Security number.

Connect with the Financial Fraud Consortium:
info@fraudconsortium.org
(405) 676-1067

- Some scammers will call you or your staff, impersonating your bank to pretend to warn you about suspicious activity on your account. They will then ask you to verify that your account isn't open or to reverse a transaction. While it may seem like they are asking you to send money back to yourself, you're sending money to an impostor.

- Fraudsters will also pose as legitimate businesses and ask for a P2P payment for their product or service. However, once you transfer your money, they won't send anything back to you and will immediately disappear.

- A con artist may also send you money by "accident" using a P2P service, where they will then ask to get that money back. However, instead of sending the money back, be sure to contact the P2P service regarding the error. If you send the money back, there's a chance that they are stolen funds; the P2P service may flag it as fraud and hold you accountable.

No matter what you do, never share your information when you encounter any of the scenarios above. A scammer will always use your details and information to create a P2P account, get access to your apps, and steal your identity.

Conclusion

While it may not impact your business yet, it may still be helpful in the long term to include information on P2P scams in your internal technology training, internal bulletin boards, or a part of the onboarding process.

Connect with the Financial Fraud Consortium:
info@fraudconsortium.org
(405) 676-1067