Consumer Advisory: Protecting Yourself Against Mobile Payment App Scams

Mobile payment apps can easily send fast money to other people – splitting a dinner check with your friends, sending emergency money to your children, paying for merchandise or a service, or even buying stocks and cryptocurrency. They can eliminate the need for you to carry cash, and are often easier to use than swiping a bank card. But the ease and convenience of mobile payment apps is also the reason they are susceptible to thieves and scammers. These apps don't generally offer the same protection as other payment methods. So, if you do use them, inform yourself about the risks and exercise good practices for protecting your money. Some of the most popular mobile payment apps include Cash App, Venmo, and Zelle.

If you are defrauded into sending money using a mobile payment app, your bank may not refund the lost funds. This is because, in many cases, the victim has "authorized" the transfer, even if they were tricked into doing so. Laws concerning the definition of "authorized" when it comes to electronic transfer of funds are murky (for information on federal regulations regarding electronic fund transfers, visit the Consumer Financial Protection Bureau). The best approach to using these apps is to treat any transferred funds as you would cash.

Mobile payment apps are a favorite tool for scammers, especially romance swindlers and cryptocurrency fraudsters. But scammers can impersonate any number of contacts you may have and trust, including banks and creditors, friends and family, employers, "tech support," government agencies, or even payment app "representatives." Don't send any money unless you know the person to whom you are sending the money, and have confirmed the authenticity of that request.

Because mobile payment apps are often linked directly to your bank account, a thief could drain your funds in a matter of seconds, and you are unlikely to get that money back.

If you do choose to use mobile payment apps – and let's face it, they are convenient – you can take steps to avoid scammers:

- Don't send money to ANYONE you don't recognize, for any reason.

- If someone you do know requests money from you, call that person to confirm that they indeed made that request to you, even if you've sent them money through the app before.
- Never give anyone access to your account, even if they tell you that they need access to fix a problem or help you recoup lost money.
- Don't feel obligated to share your contact lists with the app. If the idea of the app having access to your contacts makes you uncomfortable, deny that access.
- Regularly review statements for any bank accounts linked to the app. Contact the bank and the app customer service if you see any transactions that you didn't authorize. IMPORTANT NOTE: Many mobile payment app customer services are notoriously difficult to connect with. Many apps do not have telephone numbers, but require you to contact them through email, text, or chat platforms. This means that simply performing an internet search for an app's customer service contact information can lead you right into a scammer's trap. Always use the app or the app's official website, if there is one, to contact its customer service.
- Set up two-factor authentication on your app.
- Secure your mobile devices at all times. If you provide access to your mobile device and someone, without your permission, transfers money to themselves using your mobile payment app, you could be responsible for the withdrawal.

If you purchase merchandise or a service using a mobile payment app, and are dissatisfied with the product, contact the business to see if you can resolve your complaint. If you aren't able to resolve your complaint to your satisfaction, the Attorney General's Consumer Protection Division may be able to mediate on your behalf. You can file a complaint through the Attorney General's website, www.MarylandAttorneyGeneral.gov, or email consumer@oag.state.md.us or call 410-528-8662 (en español 410-230-1712) for assistance.

If you are scammed or tricked into transferring money using a mobile payment app, your options are, unfortunately, limited for recouping that money. But you should report the fraud to your financial institution as soon as possible. You also should report the scam to help investigators track these crimes. You can report the scam to the app's customer service, the Consumer Protection Division, and the Federal Trade Commission.

Additional Resources

- Office of the Commissioner of Financial Regulation, Maryland Department of Labor, Consumer Resources
- Consumer Financial Protection Bureau
- National Consumer Law Center, Fintech, Electronic Payments and Remittances