

Person to Person (P2P) Payment App Safety



Payment scams involving Venmo, Zelle, PayPal, Cash App, and other P2P apps have recently skyrocketed. Educate yourself by learning how criminals typically take advantage of people:

As with many scams, this one is based on the claim that the scammer is trying to protect the victim from fraud.

1. The potential victim receives a text that appears to be from their bank asking if they attempted a Zelle transaction. Regardless of how they answer, the individual next receives a phone call from the scammer, who spoofs the number so it shows up as coming from the target's bank.

2. The victim will then receive a set of instructions that ultimately winds up compromising their bank account information. The scammers use the information to withdraw funds and make off with their ill-gotten gains.

Source: *Consumer Affairs*

We're here to help! Please let us know if you have any questions or if you receive a phone call, text or email that raises your suspicions. Call 816-931-4060 during business hours, or email us any time through our [online contact form](#). We know you have many choices in banking – we are honored you choose us.

Note: By clicking links within this document you are leaving the Country Club Bank website.

More fraud information from the FCC
(Federal Communications Commission)

Home | Consumer
As More Consumers Adopt Payment Apps, Scammers Follow

The COVID-19 pandemic has altered many of our routines, including the ways we pay. Consumers are increasingly using the convenient payment options to keep themselves and families safe. As a result, the use of peer-to-peer (P2P) mobile payment apps such as CashApp, Venmo, and Zelle is growing.

P2P apps are designed to simplify financial transactions between people who know and trust each other. Like getting the check at dinner or sending utility bill payments to a roommate. Some apps have even added more traditional financial services such as debit cards and routing numbers. However, unlike traditional banks and credit cards, payment app services often lack the same fraud protections.

As Americans grow more comfortable using these apps, scammers have adapted their tactics to take advantage of the ease and often anonymous access to cash that they provide. Many of the scams look like bank alerts. Scammers may show up for the money to be sent using a P2P app instead of a gift card, an established form of scammer.

Most of the P2P apps expressly warn customers to avoid using P2P payments for purchasing goods or services. Some fraudulent consumers can get away by creating an alternate phone number or misquoting a support representative, resulting in the funds going to the wrong person. Once the funds are transferred, the money is nearly lost.

Some scammers are using for fake charitable donations using P2P apps. Before donating with a P2P app, always check the charity's website to verify that they accept donations through that app. Learn more about charity scams.

For in-person transactions, look into contactless payment options that use your mobile device or your existing credit cards.

Scam Warning
As online shopping increases, so do delivery notification text calls and texts. Find out what to watch for.

Providers Warned
The FCC and FTC demand gateway service providers do their best to help consumers catch robocalls or face serious consequences. Learn more.

Consumer Information
The FCC, COVID-19 Consumer Guide has information about consumer scams and how you can avoid becoming a victim, along with advice for an cell phone hygiene and optimizing your home wireless network, and more.