Peer-to-Peer Payment Scams

What do people who love puppies, video games, and delivery services have in common?

All are potential **targets of a rising scam utilizing P2P** (peer-to-peer or person-to-person) payment services like Venmo, PayPal, Apple Cash, and Facebook Pay.

Making matters worse, **it is extremely difficult to recover funds** once a **P2P** payment has been sent – it's like giving someone cash.

Here's what you need to know to keep from falling victim to this scam.

How P2P scams typically play out

Say you're looking for a concert ticket, video game, or someone to run errands for you. You spot a deal online – like a Cheney Facebook group or on Spokane Craigslist – and the seller asks you to submit your payment via a **P2P** platform.

Whether you have that platform or not, the **seller explains it's convenient way to transfer funds** from your bank account or credit card to their account using your internet or phone. If you don't have the platform, the seller may direct you to the **P2P** app (others not yet mentioned include Google Pay, Zelle and Cash App). You set everything up, enter the transaction amount and the seller's username or number, and press send.

And that's when the seller disappears. The money is collected, and the good or service turns out to be a hoax.

Why you could be a target of a P2P scam

A 2020 AARP survey found that while usage is most common among tech-savvy young adults, **over 70% of Americans use P2P payment services,** including 57% of the over 50 years old.

Anyone who shops **want ads is a potential target.** That's because you are more vulnerable to a scam when you are the one searching out the good or service.

"*It's easier for our members to fall victim because usually the service or goods being offered is something that the fraudster knows will catch the eye of the general public,"* warned Fabiola Garduno, a fraud specialist with a major credit union. *"The deal is too good to be true, and it is usually presented as an act now or lose out. The fraudster then pushes the cardholder to pay via **P2P** only, which is essentially like paying with cash. Once the money is transferred, it is gone."*

Be warned the next time you are browsing for a deal on an item such as an iPhone, Xbox, or video game or looking for someone to deliver groceries, meals, or run errands for you. **If the seller asks you to pay with a P2P service, it is often a scam.** Unless you have already received the item or service and are sure of the seller's legitimacy, don't send a **P2P** payment.

Can you get your money back in a P2P scam?

That's truly the (fill-in-the-blank) – dollar question. And the answer is usually no.

Scammers love **P2P** because **any dispute you initiate goes to the P2P service and not to the fraudulent seller, making it difficult to challenge.**

*"The point of the transaction from the perspective of the **P2P** payment service was to move funds, and they did what they were supposed to do,"* Garduno said.

That's not to say the fraudster shouldn't be held responsible; it simply means **P2P transactions leave the buyer less protected.**

If you do fall victim to a **P2P** scam associated with your CFCU account or credit card, reach out to us immediately at **509.235.6533** or **stop by a branch** to file a dispute.

Our goal is to try and recover the funds for our member in any way we can. Unfortunately, there are certain situations where the financial institution cannot recover them due to certain rules and regulations that are in place.

Victims are also encouraged to **file a complaint with organizations** intent on protecting consumers and prosecuting scammers for their crimes. The Washington Office of the Attorney General, Federal Trade Commission, and the Better Business Bureau all have links to file a complaint on their website home pages.

Four tips for P2P success

1. Triple-check recipients

With **P2P**, a simple mistake can cost you. Since **P2P is the equivalent of giving someone cash**, it is extremely important you only send money to someone you know. If you send money to the wrong person, that money is gone, and you cannot get it back.

2. **Avoid red-flag sellers**

Typically, a fraudulent seller will use terms like “act now or you’ll miss out” or may otherwise come off as pushy. They **may also be insistent on payment through P2P** and resistant to other transaction methods. If you feel hurried or get a sense the offer could be too good to be true, those are major red flags. **Before you send the money, look out for any last-minute changes in the goods or services you are paying for.** Fraudsters are known for add-ons such as purchasing insurance for a high-value transaction in order to maximize their return per scam victim.

3. **Set up added securities**

P2P platforms typically allow a user to create a PIN or similar protection that is required when opening the app or transferring money. This extra layer of security protects you if someone else gets access to your phone.

4. **Send to people you know**

P2P systems aren’t intended for online purchases or other transactions with strangers. They are **designed to be used among friends and known associates,** such as helping to cover a restaurant tab or paying a trusted babysitter or hairstylist.

P2P for the Win!!

Remember, scammers shouldn’t keep you from using the latest technologies. In fact, **we’ve been offering Member to Member transferring at CFCU for a while now- FREE,** just call us and with permission from both account owners we can give access for transferring funds.

The key is to **stay informed, follow best practices, and trust your instincts when something doesn’t feel right.** When used properly, **P2P** can be an excellent option for 21st century transactions.