Paying the Price of Trust: Peer-to-Peer Payments

Center Forward Basics

March 2025

Overview

Peer-to-peer (P2P) payments are digital transactions allowing individuals to transfer funds directly to one another using electronic platforms or applications. These services enable users to link their bank accounts, credit cards, or digital wallets to swiftly send and receive money. Popular P2P platforms include PayPal, Venmo, Zelle, and Cash App. To sign up for one of these apps, users can either enroll in an eligible bank account or create an account through a P2P platform that can be funded by a bank account, debit, or credit card.

These payments use a recipient's phone number or email address linked to their P2P account to send funds quickly. Services are often free for transferring funds between P2P accounts or linked bank accounts, but occasionally, providers require fees of about 3% to process a credit or debit card. Money exchanged in P2P payments can typically be used immediately when sent through a bank account or in an app. For P2P services that aren't directly linked to a bank account or digital wallet, money is typically available within one to three business days. Consumers often use P2P payments to split restaurant checks, pay friends back, etc.

Payments Fraud

As the adoption of P2P payment systems has grown, so too have concerns regarding fraud and scams. Payment fraud involves illegally obtaining financial information, with consumers often unaware. Scams occur when a bad actor tricks a consumer into sending money or giving away bank information of their own volition. Examples include scammers posing as banks or businesses and convincing consumers to send money or share their account information because their account was frozen, there was suspicious activity on their account, or any number of lies. Like cash, P2P payments are quick and easy to exchange with someone but difficult to get back once funds are sent.

Current Safeguards

To address the growing concerns around fraud and scams in P2P payment systems, platforms and financial institutions have introduced various safeguards. It is important to distinguish between scams and fraud, as the two require different responses. Scams occur when consumers knowingly authorize a payment under false pretenses, often after being deceived by bad actors. These cases are challenging to resolve because the customer technically authorized the payment. Fraud, conversely, involves unauthorized transactions where the consumer's account or payment information is used without their consent. In these instances, banks are required by law to reimburse customers, ensuring some level of protection against financial loss.

Although scams are more challenging to combat than fraud, banks and P2P platforms have implemented various measures to mitigate their impact. For example, P2P services like Zelle providers provide in-app safety alerts and real-time account monitoring. Consumer education also plays a critical role in these efforts. Financial institutions, often in partnership with

Center Forward Basics

Center Forward brings together members of Congress, not-for profits, academic experts, trade associations, corporations and unions to find common ground. Our mission: to give centrist allies the information they need to craft common sense solutions, and provide those allies the support they need to turn those ideas into results.

In order to meet our challenges we need to put aside the partisan bickering that has gridlocked Washington and come together to find common sense solutions.

For more information, please visit www.center-forward.org

government agencies, run campaigns to teach users how to identify potential scams, such as phishing attempts or fraudulent payment requests, and how to respond appropriately. Educational resources, including online guides and interactive tutorials, are readily available to help consumers understand common scam tactics and adopt best practices to protect themselves. By empowering users with knowledge and tools, these initiatives aim to reduce the risk of falling victim to scams and enhance overall trust in P2P payment systems.

Current Legislation and Regulation

The Electronic Fund Transfer Act (EFTA) of 1978 was designed to protect consumers engaging in electronic fund transfers (EFTs), including transactions made via ATMs, point-of-sale terminals, and automated clearinghouse systems. This foundational legislation ensures consumers are shielded from unauthorized transactions and provides a framework for addressing errors and disputes. However, as the frequency and complexity of fraud and scams have evolved, the EFTA's provisions may need to be updated. One proposal being considered; which was introduced by Senator Richard Blumenthal (D-CT), Senator Elizabeth Warren (D-MA), and Representative Maxine Waters (D-CA) in August 2024; is the Protecting Consumers from Payment Scams Act. This proposed legislation aims to update the EFTA's protections to P2P payment users and requiring platforms to take greater responsibility for preventing and addressing scams.

On the regulatory side, the Consumer Financial Protection Bureau (CFPB) enforces the EFTA through Regulation E, which outlines the responsibilities of financial institutions in cases of unauthorized electronic transactions. Regulation E requires banks to investigate reported errors and fraud within 10 business days and to provisionally credit affected accounts during investigations. The current version of Regulation E was not specifically designed with P2P payment platforms in mind, leading to ambiguities in how its rules apply to newer technologies and practices. To address this, the CFPB proposed a rule toward the end of President Biden's administration to expand oversight of digital payment platforms. This rule mandates more straightforward disclosure requirements, enhanced fraud prevention measures, and increased accountability for platforms in resolving disputes and compensating consumers for unauthorized transactions. These regulatory updates reflect a growing recognition of the need to protect users in an increasingly digital financial landscape, balancing innovation with consumer safeguards.

While these updates aim to protect consumers, they also raise concerns about unintended consequences. Expanding Regulation E to P2P platforms could make it easier for scammers to exploit reimbursement policies, complicating fraud prevention. Unlike traditional banks with established fraud protections, P2P services act as intermediaries, creating uncertainty over who is responsible when issues arise — the bank or the platform. Without clear liability rules delineating responsibility, banks and P2P service providers could face business disruptions and complicate, rather than benefit, consumer protections. Additionally, expanding consumer protections to scams could complicate the viability of P2P systems. An increase in the regulatory burden for P2P payment systems has the potential to disrupt the ease of access and use of P2P systems, key functions that attract users to P2P systems.

The evolving landscape of P2P payments necessitates a balanced approach, ensuring consumers benefit from the convenience of these services while being shielded from potential risks. Ongoing collaboration between regulatory bodies, financial institutions, and technology providers is essential to maintain the integrity and security of P2P payment systems.

Links to Other Resources

- Bank Policy Institute – Online Fraud Is Real, But Zelle is a Safe Harbor, Not the Problem;
- Bank Policy Institute – Some of the Many Ways Banks Keep Zelle Customers Safe
- Federal Bureau of Investigations – FBI Tech Tuesday: Beware of Scams on Popular Peer-to-Peer Payment Apps
- Federal Reserve – Electronic Fund Transfer Act
- Forbes – Attacking Banks For P2P Scams Is A Non Sequitur In Search Of A Fix
- Reuters – US consumer watchdog probes major US banks over Zelle scam, WSJ reports
- Journal of The James Madison Institute – Fraud, Scams, and the Case for Accountability in Third-Party Payment Platforms