

P2P Payments are Rising and So is Fraud

Cashless, online transactions are increasing. That's no surprise. We all saw it coming, and with a global pandemic introducing a new reason to go cashless, digital money transfers are now more popular than ever. Also forecasted – and moving just as quickly as consumers' acceptance, unfortunately – is fraud in this space.

Accelerated by the rise in cashless payments, fraud has found increased opportunity in peer-to-peer (P2P) payment platforms like Cash App, Venmo, Zelle and others. Using a P2P payment app, users can send money to other individuals and businesses, bypassing the ATM. The convenience of sending money via a personal device, amplified by pandemic-related social distancing mandates, has led to an explosion in P2P use.

A P2P payment account facilitates the transfer of funds from a smart device by linking to a user's account with a traditional credit union or other financial institution. Once linked, the user is free to send and accept funds via their "wallet." Fraudsters have exploited this ease-of-use, leveraging P2P apps to create wallets with stolen account information. When a fraudulent profile is created, the fraudster is free to drain the balance directly via transfer, unbeknownst to the actual account holder. Transaction data tells a dramatic story of the increase in P2P payments fraud. For example, based on FIS' fraud tag data, Cash App had over 107.5 thousand confirmed fraudulent authorizations attempted in 2020, experiencing its sharpest spike in April, for a total of more than \$12.7 million.

It's at the point of P2P payment account activation that most fraudulent attempts are made, explains David Adams from FIS Fraud, Risk and Compliance Solutions. Once a fraudulent account has been created, the criminals are trying to drain the balance as quickly as possible before detection.

"For fraudsters, it's really a race against the clock," David says. "Once they have set up a profile with stolen credentials, the timer begins, and they act quickly so they can empty the account and cash out their P2P wallet."

Last year, FIS' fraud-prevention tools analyzed over 54 million Cash App authorization attempts worldwide totaling more than \$4.8 billion, a huge increase from 2019. Other P2P payment platforms experienced similar growth. At FIS, the Fraud Analytics team has stepped up their game to get out in front of the fraudsters, implementing several sophisticated, global strategies to identify and prevent fraudulent activity as early as possible.

"Our goal is to stop fraud before it even begins," David says. "Leveraging our logic-based rules engines, we've been looking at this activity in completely new ways to identify correlations between the risky transaction behavior. It takes quite a bit of research on our end, but we're confident it will pay off."

Since April 2020, attempted fraud amounts in the P2P segment have stayed at increased levels, David reports. And as the fraudsters employ new devices for pirating member account information like automated bot technology, he says, FIS is committed to staying ahead of the next fraudulent scheme.

"With COVID-19 accelerating shifts in purchasing behavior to card-not-present, we believe peer-to-peer payment fraud is here to stay," David says. "This is a top priority for the FIS Fraud Analytics team. Our goal is to protect our clients and their cardholders and to make the fraudster's job as hard as possible."

To learn more about FIS Fraud Analytics or any FIS product, please contact Lisa Slaymaker at lslaymaker@mwcua.com.