ACAMSTODAY.ORG

ACAMS TODAY™

# Preventing Digital Payment Systems Fraud


Digital payment volumes have increased dramatically during the COVID-19 pandemic as more companies sell their products and services through digital channels. These payments have expanded to new areas, such as grocery deliveries, vacation rentals as well as automotive sales and repairs. In addition, more consumers make purchases through mobile apps and digital wallets.

What is more, customers prefer merchants that offer digital payments and the growth in digital payments shows no signs of slowing down. In fact, according to a global study from the market research firm Leger and payment provider Blackhawk Networks, 63% of consumers say they are more likely to shop at a retailer that accepts digital payments.

ACAMS

Reprinted with permission from acamstoday.org

A publication of ACAMS®



genpact


## Criminals Are Exploiting the Boom in Digital Payments

Unfortunately, the surge in digital payments has also attracted fraudsters determined to illegally profit from this trend. As providers adopt and scale digital payment capabilities to match its demand, it is critical that they prevent fraud and reduce losses while minimizing customer friction.

Providers must have a good grasp of the tactics that criminals are using. These tactics fall into several key areas, including:

### *Peer-to-Peer Fraud*

There is fraud involving popular peer-to-peer (P2P) payment apps, such as Venmo, Zelle and Cash App, which frequently occurs through social engineering and scams. Some of the scams include fake merchandise and fake charity donations as well as account takeovers, which involve customer information obtained through the dark web or through malicious bots. Fraudsters use stolen identity information to apply for new P2P and digital wallet accounts and then use those accounts to purchase goods and services.

### *Authorized Push Payment Fraud*

Authorized push payment fraud is another fraudulent technique that occurs when scammers pose as legitimate businesses or government officials to trick victims into transferring funds to them through real-time digital payments.

### *Friendly Fraud*

Friendly fraud is also on the rise. This involves a user disputing a valid transaction, or a user's mobile apps and logins being used by friends and family members without permission. A provider's security features cannot stop this type of fraud and merchants often do not have enough information to track and validate the transaction, so chargebacks typically go through successfully and merchants bear the cost of refunding the money to consumers.

There is a lot to think about. So, how can providers stay ahead of fraudsters while keeping up to date on emerging threats? The good news is that the technology behind digital payments is inherently secure, specifically digital wallets and P2P payments.

### *How to Protect Your Digital Payments Systems*

The key is in designing a solution that uses data to stop fraudulent activities. This involves four steps:

1. **Use a cloud platform.** Using a cloud platform to enable robust data ingestion and enrich data from multiple sources would provide a broader spectrum of real-time data, enabling faster analysis, real-time fraud detection and more accurate fraud decisions.
2. **Examine the entire customer lifecycle.** Gather centralized data intelligence holistically, in real-time, at each customer touchpoint, from application, transactions to account updates and from device data to behavioral data. This will help quickly identify evolving fraud patterns.
3. **Use intelligent authentication.** Depend less on passwords and use secure, frictionless methods for intelligent customer verification and authentication. Modern-day fraud verification and authentication incorporates advanced digital technologies, such as artificial intelligence, machine learning, and biometrics (fingerprint, facial and voice recognition) as well as dynamic data for customer verification and authentication.
4. **Preserve the customer experience.** Customers can quickly switch to other digital payment providers if they experience slow transactions or feel that their current process is too complicated. Building a seamless fraud-detection process that is invisible to customers requires optimal prioritization between growth (e.g., approval rate) and fraud rate.

## Conclusion

The struggle against fraud has no end. But providers that harness data and use advanced digital technologies to develop a deeper understanding of their customers will have an advantage in keeping fraudsters out, ensuring that digital payment continues be a favorite of consumers and providers alike. AT

*Brian Baral, global head of financial crime risk management,Genpact, LinkedIn*

*Joseph Gillespie, global practice leader of financial crime risk management, Genpact, LinkedIn*