JAVELIN

Securing P2P Payments

01 July 2020 By: John Buzzard, Krista Tedder

Person-to-person (P2P) payments continue to flourish in the United States as more consumers adopt faster payments as a way to deal with busy, digitally infused lifestyles. The P2P payment grid across the span of product providers and participating financial institutions has started to exhibit signs of vulnerability. Fraud drivers such as account takeover, consumer misuse, and money laundering have reached a critical mass. Lagging investment in enterprise fraud management tools and a misunderstanding about who is responsible for P2P fraud are at the heart of the problem.

Recent societal changes spurred by the COVID-19 pandemic, such as social distancing and self-quarantine, are reshaping payment behavior worldwide. Payment transaction volumes are shifting into contactless and card-not-present channels to bridge the gap of in-person transactions. There will be significant criminal exploitation within the P2P grid during this period as consumers struggle to adapt to material shortages and isolation.

Key questions discussed in this report:

- What fraud threats are consumers and financial institutions facing today?
- Are fraud detection and prevention technologies meeting the current needs of the P2P payment grid?
- How can financial institutions layer on technology to increase authentication and reduce future P2P fraud?

The 2019 ID Fraud survey was conducted online among 5,000 U.S. adults over age 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place from October 22 through November 4, 2019. Data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100