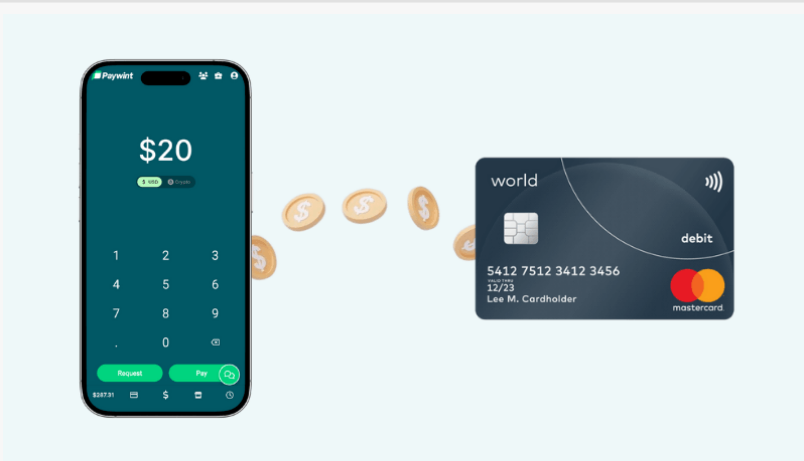
Paywint Forecasts Surge in Push-to-Card Fraud as U.S. Fintech Adoption Accelerates

A measurable fraud shift is reshaping U.S. fintech as instant push-to-card payouts compress decision windows, demanding faster, smarter fraud response.



Push-to-card (OCT) transaction flow showing real-time digital wallet payout to debit card infrastructure.

TYLER, TX, UNITED STATES, February 23, 2026 /EINPresswire.com/ -- According to 2026 reports by fintech leaders, push to card remains the most popular transaction type for enterprise senders, with nearly 20% adopting the model. Similar studies show the rising trend in push-to-card transactions. It could create more fraud, deception, and illegal activities. Fintech leaders like banks, digital wallet providers such as Paywint, and top finance operators are working aggressively to forecast fraud in the push-to-card and Original Credit Transaction (OCT) space. The collective goal is to understand and analyze push-to-card fraud risks and take corrective measures to empower the US fintech market.

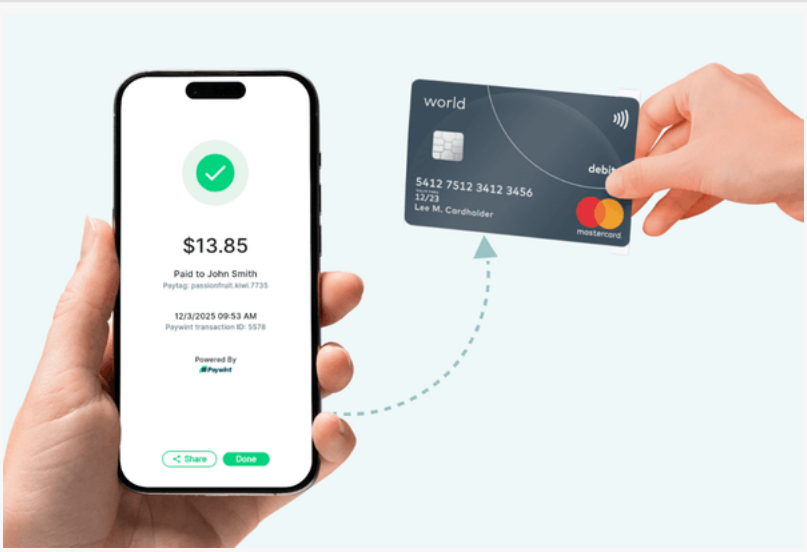
> Push-to-card growth must be matched with real-time risk intelligence. Speed without adaptive fraud controls exposes fintech ecosystems to escalating, AI-driven financial threats."
>
> *Dr. Saheer Nellil*

Why Push-to-Card is Prone to Fraud

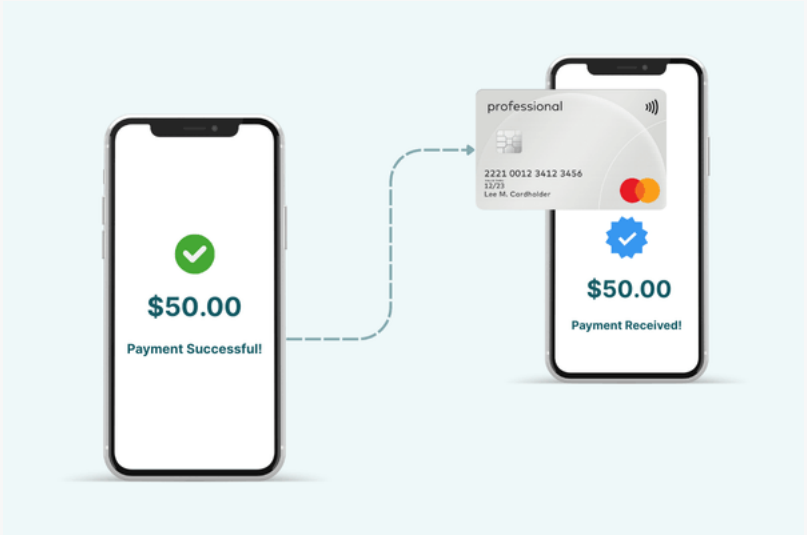
Push-to-card or OCT finds wide applications in gig economies, contract payouts, marketplace earnings, wage and payroll disbursements, insurance claims, refund models, reward programs, and small-scale business services. This attracts all sorts of target consumers seeking instant payment support.

The payment infrastructure also attracts fraudsters and deceivers for the same reasons. Deloitte industry insights state that authorized push payment fraud could surge to $15 billion by 2028. It's hard to visualize these numbers in practice, owing to the perceived damage to the fintech-oriented segments.

Instant payments reduce settlement times. Faster payouts mean the time available is lower for conducting real-time checks. Fraudsters and digital impersonators can drive push payment losses. The transactions might seem legitimate and can even deceive seasoned fraud teams and compliance professionals.



Instant push-to-card payout confirmation showing real-time transfer from digital wallet to debit card.



Successful push-to-card payment showing real-time fund transfer and instant settlement confirmation.

Push-to-card payment rails present high exposure to fraud attacks and attract scammers and money mules alike. Some of the general fintech frauds, like social engineering and authorized push payment (APP) scams, occur in this scenario as well.

Main Reasons for Push-to-Card Fraud Surge:

Fast and Irreversible Rail
Chance for Victim Authorization of Fraud
Capacity of Fraudsters to Overcome Efficiency Gaps
Exploitable Onboarding Functions in OCT
Scam-driven Intent in Payouts
Compromised Money Movement

Forecasting Push-to-Card Fraud Patterns

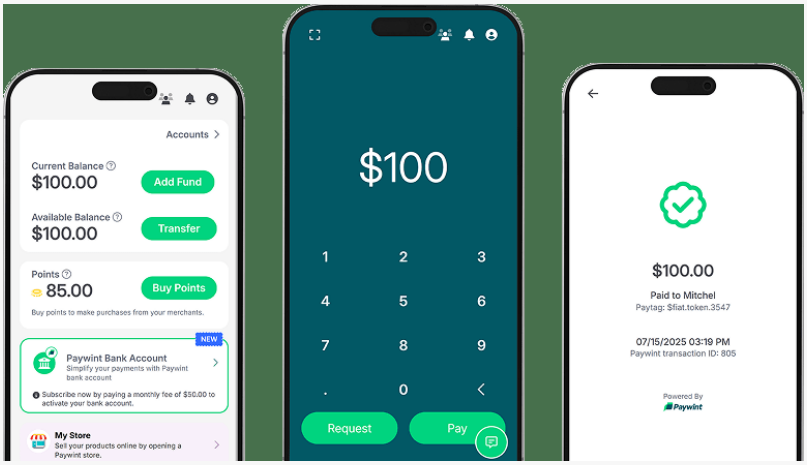
As the push-to-card volume increases, fraud shift might pose an even bigger risk with specific patterns to observe. The fintech industry - layered with fintech providers, digital wallet providers such as Paywint, and banking systems - can expect those in:

Mule Accounts

Intermediate parties will create mule accounts based on control of cards and card-linked points. Fraudsters recruit people to receive illegal funds, and the transfer supports illicit cash storage. The push-to-card model will be explicitly used to create fraud with this cash flow and money movement. Fintech instruments should be aware of mule accounts operated by fraud rings.

Instant Refund Fraud

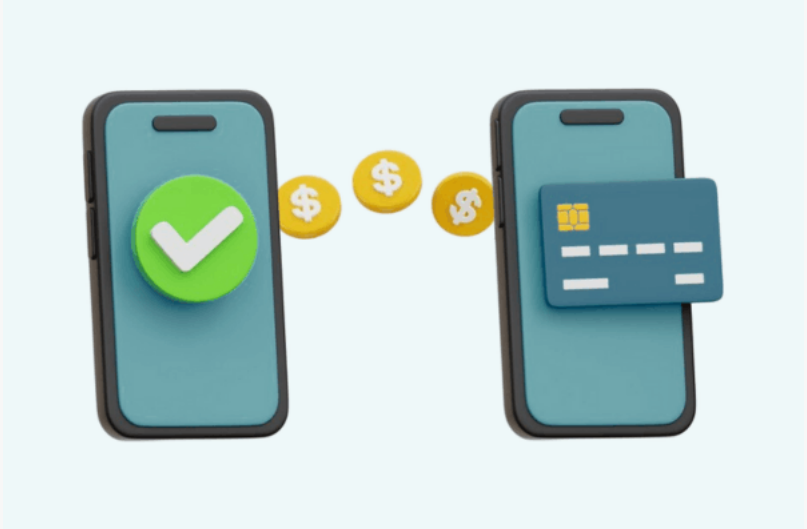
This type of fraud exploits time delays between a card payment's approval and settlement. It might be visible only during the payment reconciliation process. It is part of internal fraud activities where the fintech transactions could be disputed that seems like legitimate behaviour.



Mobile fintech dashboard showing fund management, push-to-card transfers, and instant payment confirmation.

APP-style Scams

Authorized Push Payment (APP) fraud and scams are part of social engineering, where victims are deceived or persuaded into transferring funds. In a push-to-card rail, the manipulation happens with the criminals initiating a card payout with the victim's approval. Quick money movement makes it hard to detect, pause, or stop the transaction.


Secure push-to-card transaction showing real-time payment processing and instant card settlement confirmation.

User Account Takeover

A recognized fraud pattern set to continue its problematic rise is account takeover. In push-to-card models, the fraud rackets operate a structure where user accounts are compromised with phishing or malware practices. From here on, they can change the card payout details and trigger instant card transactions or transfers. The time to detect and review this anomaly is comparatively shorter while pushing the money to debit, credit, or other prepaid cards.

Payout Promises

These come under the tag of APP attacks. The scam could narrate false promises, urgency tricks, pressure tactics to create fake relevancy, and upfront fee fraud to unlock potential earnings that are absent in reality. These risky tactics are employed by fraudsters to directly reach out to genuine customers with cards and conduct the crime. Voluntary participation in large numbers makes it harder to recognize a fraud pattern.

Generative AI Tricks

With Generative AI (GenAI) tools and resources, financial criminals can create deepfake techniques in voice, documentation, and automation. These could scale in attack as their distinguishing features from the legal structures are minimal. Alert pattern recognition and groundbreaking technology innovation can contribute to challenging AI's negative impact.

Industry Response Through Leading Fintech Networks

Push-to-Card payment solutions are meant to define the financial transactions of a business with speed, safety, control, and convenience. Effective fund management and instant settlements can drive the business model operations forward.

Responsible ecosystem partners like Paywint align sincerely with the fintech operators, businesses, and compliance authorities to dynamically enhance the OCT niche. Fraud control and scam-risk assessment are fruitful in models opting for relevant parameters.

As real-time payment fraud threats evolve, continuous monitoring and dynamic risk scoring become essential safeguards. These also cover identity signals for fraud alerts and cross-entity intelligence to tackle the scam. Rather than the critical decision-making perspective of a single entity, what matters is the collaborative approach towards fraud defense.

Fintech leaders like Visa and Mastercard follow unique measures to empower fraud prevention tactics on their cards. Visa provides insights with name-matching services to reduce account takeovers. Mastercard showcases AI measures to identify and remove mule accounts with real-time detection and scoring.

Overcoming Push-to-Card Fraud without Losing the Rail's Identity

Push-to-Card or the OCT niche is gradually on the rise. Issues related to fraud and scams shouldn't derail the system's growth. In fact, fintech solutions should prioritize and deliver a model that marries speed with safety. Risk adaptability in push-to-card transactions can be facilitated with:

Maintaining a beneficiary graph to distinctly identify and classify recipients to analyze the risk.

Adding step-up controls by deploying solid passkeys, account cool-down windows, re-authentication factors, and identification structures for device, timing, amount, etc.

Enabling velocity rules to operate across device clusters, IP ranges, and recipient rules, and thereby tackling fraud operations.

Designing customer support prompts to generate scam awareness by offering insights with contextual warnings, support playbooks, etc.

Closing the fraud and scam loop with adaptive friction, where beneficiary trust is made measurable.

At no point should the confirmed scams, disputes, and chargebacks be neglected in adding to the detected fraud pool. Pattern recognition should be embraced as a highly effective tool to correctly forecast and overcome the fraud surge.

Leadership Perspective

As per Dr. Saheer Nelliparamban, Founder and CEO of Paywint LLP, “A shared financial ecosystem with real-time risk intelligence monitoring is the most effective way to tackle fraud in Push-to-Card payments. The future is about embedded finance tactics with secure scalability for fintech partners. Paywint’s payments infrastructure strategically mitigates the risks in push-to-card transactions.”

About Paywint

Paywint is a U.S.-based digital wallet and payment platform focused on enabling small and medium-sized businesses to access funds instantly and manage financial operations more efficiently. The platform provides secure, real-time settlement capabilities alongside tools for payments, payroll, invoicing, and transfers. Paywint works with regulated banking partners and global payment networks to ensure compliance, security, and accessibility for businesses across multiple sectors.

Saheer Nelliparamban
ZilZil LLC d/b/a Paywint
+1 (408) 831-1412
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube

X