APP Fraud

Today's fastest-growing threat to digital payments

Authorized push payment (APP) fraud, P2P fraud, instant payments fraud—this scam technique goes by many names and presents an existential threat to fintechs. This isn't just because of the fines and reimbursement responsibilities that are the cost of doing business in the financial space, nor is it because APP fraud makes up 75% of today's digital banking fraud on a dollar-value basis.[1] It's because of another number: 14%.

This is the proportion of customers who trust fintechs—it's only thanks to ease of use that they employ services like Revolut, Zelle, CashApp, and others at all.[2] However, stories of fraud-heavy payments companies like these being blacklisted from interacting with other banking services altogether have lately gone from a trickle to a flood.[3] There's nothing less convenient than needing to make a payment only to find that your app doesn't play well with others, so consumers—already lacking confidence in fintechs—see no qualms about dropping one service in favor of another that gets their money where it needs to go.

In the US, APP fraud

...has victimised around 1 in 8 Americans[4]

...is on track to create $3 billion in losses in 2026–double what was seen in 2021[5]

...has appeared as a subject of Congressional inquiry

In the UK, APP fraud

...represented 41% of all fraud losses in the first half of 2022 alone, around £250 million[6]

...has already been singled out as a concern by the Financial Conduct Authority

What makes fintechs desirable is also what makes them vulnerable

Though consumers cite convenience and speed as reasons for sticking with new payments platforms, these are also the two areas most ripe for scammers' exploitation.

Convenience: fake account creation in minutes, anywhere

To deliver on their claim to provide more accessible financial services, neobanks often guarantee rapid signups without needing to visit a brick-and-mortar location. But tech-savvy criminals can systematically probe digital-only automated onboarding processes for technological gaps, then manipulate what they find with fake or stolen documents, bots built to speed-run KYC checks, and more. In the end, nearly endless, nearly risk-free attempts to create fraudulent accounts result in specialized financial criminals having access to nearly countless money mules highly concentrated within fintechs' user bases.

Speed: payments in seconds, hours to unravel

Consumers also expect their transactions to be completed instantly. However, when financial criminals have a money mule network at their fingertips, it's child's play to take the next step into money laundering by passing fraudulent funds through fake accounts to cover their tracks. Every "hop" between accounts means just seconds to attackers but complex, cooperative investigations for fraud and compliance teams, buying scammers time to reconsolidate and extract their proceeds.

This is what makes APP fraud—and the mules that drive it—an existential issue for up-and-comers in the finance space: by playing host to networks of easy-to-create synthetic money mule accounts linked together by instant payments, fintechs will disproportionately feel the impacts of APP fraud on their reputations and bottom lines. Luckily forward-thinking fintechs are also ideally positioned to implement forward-thinking safeguards against today's biggest threat: enter Resistant AI.

[1] "Authorized Push Payments Surge to 75% of Banking Fraud" (Infosecurity Magazine, 2022
[2] "The Rise of Open Banking in North America" (Mastercard, 2021)
[3] "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards" (Forbes, 2021)
[4] "The Big View: All Sentinel Reports" (Federal Trade Commission, 2023
[5] "APP fraud volumes expected to double by 2026, says report" (Computer Weekly, 2022)
[6] "2022 Half Year Fraud Update" (UK Finance / LexisNexus, 2022)

App Fraud

Filling the gaps with perpetual KYC

There's no magic wand to wave away money mules. Instead, multiple independent layers target the existence of money mule accounts as well as their activities, progressively reducing the level of threat and covering each other's blind spots throughout the customer journey.

Beyond documents: behaviors

Before customers even submit any personal documentation, Resistant AI's Identity Forensics analyzes user behaviors, form submission characteristics, device characteristics, and more to detect repeated or automated requests to create an account—clear indicators of a bad actor trying to penetrate your systems. Pre-onboarding checks alone can raise the number of identified fraud attempts by 28%.

Preventing mules during onboarding

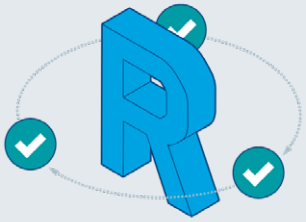
You intake customer documentation as you would normally, and Document Forensics automatically analyzes them for forgeries and serial fraud. Not only will this uncover digital alterations that fool traditional checks, it will block patterns of reused documents—as forgery templates and stolen identities often are. This helps to eliminate up to 90% of manual reviews, though our 99.2% accuracy rate still means the creation of new fraudulent money mule accounts will be effectively prevented altogether.

Clean out accounts connected by transactions

In real time, our Transaction Forensics allows you to identify behaviors consistent with the receipt, shifting, and withdrawal of fraudulent funds among money mule networks. Specially developed detectors use statistical anomalies to flag suspicious money flow patterns and relationships between accounts—relationships that point to fraudulent accounts, account takeovers, and other bad actors all working in favor of fraudsters.

Apply learning for perpetual KYC

The information our combined products have gleaned throughout the preceding steps is applied recursively throughout the rest of the protected entity's network. Documents since revealed to be forged or stolen may weed out accounts previously thought to be legitimate, while scams in progress or sleeper agents may be revealed when customers deviate from their normal behaviors.



Breaking up APP rings once and for all

The combination of insights from identity documents, non-identity documents, digital fingerprints, consumer behaviors, and transaction monitoring turns the table on fraudsters: spreading out reactions over the life cycle means they can never be certain whether the money mules they control have already been detected as potential money muling accounts or will be soon. No APP gang wants to transfer stolen cash through accounts that will be blocked the moment fraudulent proceeds reach them. This is how Resistant AI helps you break the business model of attackers, protect your institution from reimbursement costs, and preserve the low-friction financial services ecosystem your customers rely on.