

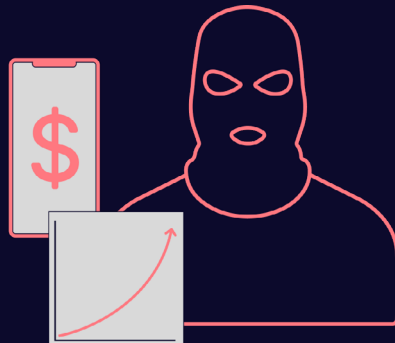
# APP Fraud & Money Mules

The greatest threat to fintechs today

## 01 Defining the problem



## 02 What's driving APP Fraud



## 03 Why—and how—fintechs must lead the fight



resistant<sub>rx</sub>ai

# Executive summary

---

To the casual observer, the relentless creativity of the fraud world has become a form of entertainment all its own: YouTubers like Jim Browning bait and trap call center scammers, *The Tinder Swindler* showed Netflix audiences romance scams taken to extremes, and sharing screenshots of half-hearted spam texts is a popular Twitter pastime. These expose how the modern technologies we all rely on for everything from communicating with loved ones to running our businesses—social media, chat apps, search engines, ad networks, and more—can also be used by fraudsters in endless variations of impersonation, purchase, and investment scams.

But regardless of the outward form of the initial scam, those paying attention will also find a core unifying element behind all the different faces of modern fraud: 75% of all digital banking fraud on a dollar-value basis involves authorized push payments (APP) on fast payment networks.<sup>1</sup> This is the new backbone of the fraud world.

The ability to both request and make direct payments combined with users' expectations of near-instant payments in legitimate settings have formed an ideal transactional environment for criminals, one nearly free of intermediaries. Victims and their funds can be parted with never-before-seen ease, while fraudsters can keep ill-gotten funds on the move, hard to track, and harder to freeze, provided they have enough money mule accounts under their control to digitally outrun investigators.

Neobanks, payment service providers, and other financial innovators are being blamed by the media and regulators for facilitating this type of financial crime and the mule accounts that execute it. The argument goes that fintechs' pursuit of reckless growth at any cost means chronic underinvestment in digital onboarding safeguards and even turning a blind eye to wrongdoing. As we'll show, this is a misdiagnosis of the problem, one touched off by misreadings of the state of play and perpetuated by traditional players with vested interests. Yet the reputational damage incurred as fintechs are scapegoated is real, as is mounting regulatory pressure.

The reality is that any financial institution built on or pivoting to a digital-first or -only strategy will face the same fraud and AML challenges. So rather than piling on fintechs and undoing the innovations they've spearheaded, we must recognize that digital-native companies have the best chance to successfully tackle the staggering problem of APP fraud—to the benefit of the industry as a whole.

This white paper aims to help forward-thinking fintechs rise to this challenge.

---

<sup>1</sup> "Authorized Push Payment Surges to 75% of Banking Fraud," Infosecurity Magazine

**SECTION 01**

Defining the problem .....	3
What APP fraud is .....	4
APP fraud in numbers .....	5
What recourse do victims have? .....	9

**SECTION 02**

What's driving APP fraud .....	10
Growth-focused business models under fire .....	11
Greater regulatory scrutiny & mandatory reimbursements .....	14
Are fintechs truly more exposed? .....	15
Are fintechs truly more at risk? .....	20
Banks, neobanks, and statistics: Traditional banks fare no better than fintechs .....	22

**SECTION 03**

Why—and how—fintechs must lead the fight .....	24
Fintechs are where the solution starts .....	25
The Resistant AI approach: Defense in depth .....	26
Steps any organization can take now .....	28
References .....	30



## SECTION 01

# DEFINING THE PROBLEM

---

To understand and ultimately fight this booming criminal activity, we first need to define what the problem is and who's taking notice.

# What APP fraud is

---

*Authorized push payment (APP) fraud is a type of financial scam wherein a fraudster social engineers—cons—an individual or business into sending money to a bank account controlled by the criminal in what the victim believes to be a legitimate transaction.*

In other words, the goal is to manipulate victim account holders into facilitating part of the scam themselves. The victim account holder personally authorizes a payment to someone they understand to be a trusted—or at least legitimate—payee, but the money is transferred to a fraudster's account instead.

## A scam by any other name

The power of this type of scam hinges on the means by which the initial transfer is made. What was once referred to as a bank transfer scam has become supercharged and rebranded thanks to mobile and real-time, even instant, payment rails that move money much faster than traditional bank transfers—with less time for controls or reviews.<sup>2</sup>

Europe, where fast peer-to-peer (P2P) payments have proliferated for some time, first noted and gave **APP fraud** the name we'll use throughout this document. In the US, where the high-profile nature of scams on Zelle took center stage, it is sometimes referred to as **P2P scam or P2P fraud**. The coming introduction of FedNow, which will be cheaper and faster to operate than ACH and wire transfers<sup>3</sup> and will provide the same kind of instant payment capabilities currently seeing more limited use by institutions employing TCH Real-Time Payments such as Zelle, will likely compound the challenge. In Canada, it is often referred to as **Interac e-Transfer fraud** due to the prevalence of the Interac fast payment system.

Since this scam technique refers to the channel used to carry it out, it's often obscured in news and fraud reports by the social engineering flavor that tricked the victim into sending the money in the first place (more on those later). But from the point of view of the institutions handling the money, all of these boil down to one core component: how the money is moved.

---

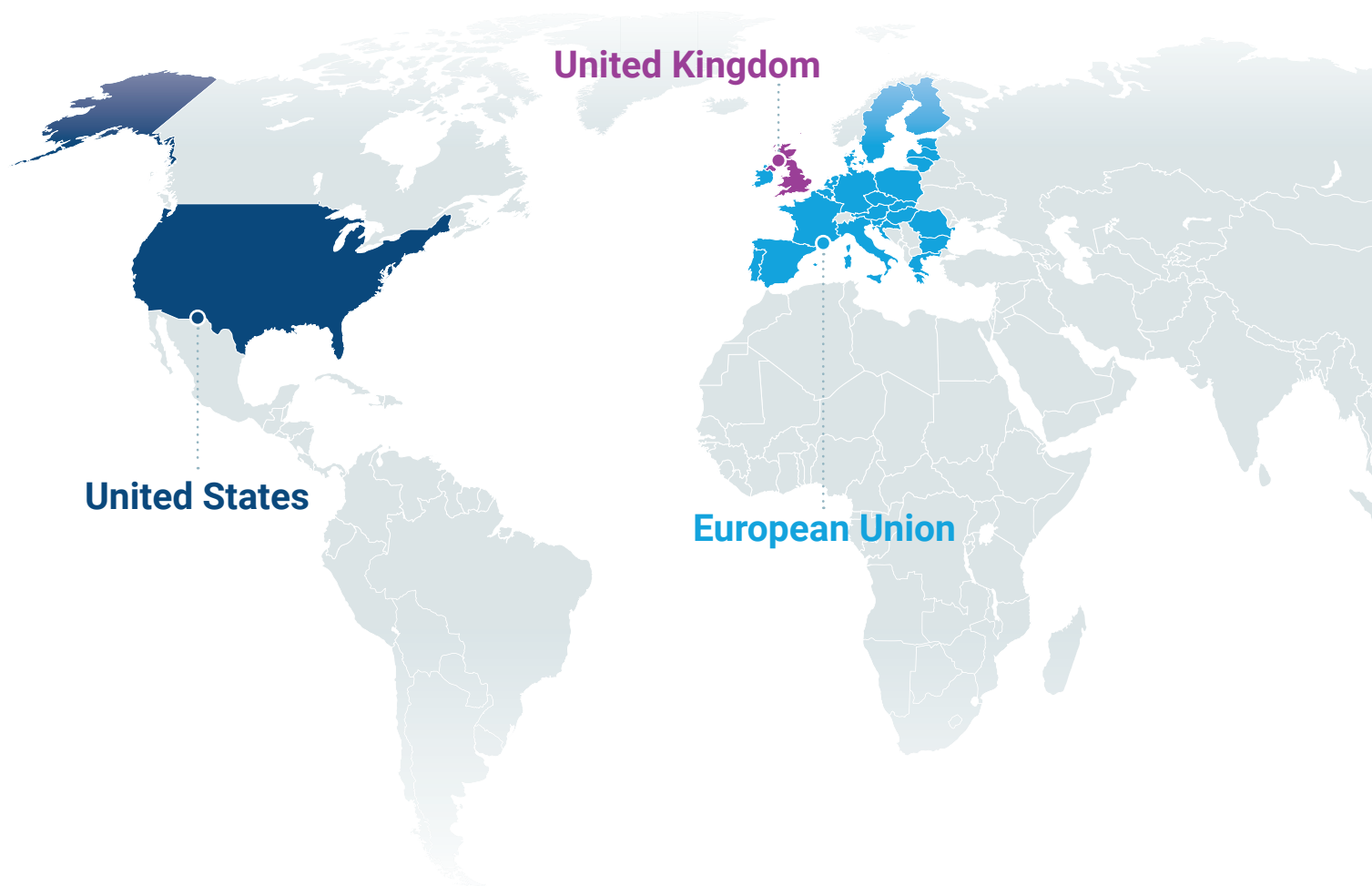
<sup>2</sup> "Discussion Paper on the payment fraud data received under PSD2 (EBA/DP/2022/01)—Submission #10," European Banking Authority

<sup>3</sup> "Fed's Zelle-like instant payment system to go live in July, hundreds now testing," Computerworld

# APP fraud in numbers

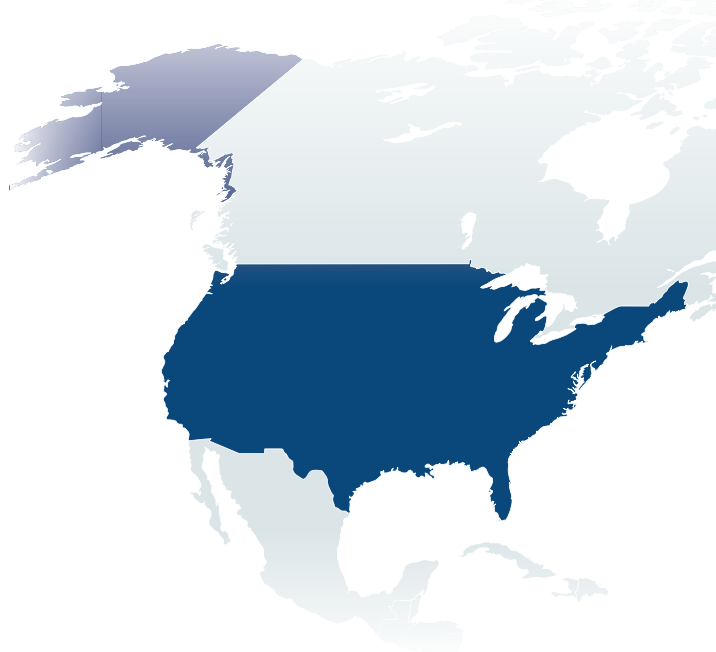
Other than using cryptocurrencies, APP fraud is quickly becoming the go-to mechanism for criminals of all kinds to power a whole galaxy of scams. This is reflected by its rapid growth:

- Globally, APP fraud represents 75% of all digital banking fraud on a dollar-value basis.<sup>4</sup>
- Authorized push payment fraud losses in the US, UK, and India are expected to double in the next four years, hitting \$5.25 billion by 2026 with a compound annual growth rate of 21% across the period.<sup>5</sup>



<sup>4</sup> "Authorized Push Payment Surges to 75% of Banking Fraud," Infosecurity Magazine

<sup>5</sup> "APP fraud volumes expected to double by 2026, says report," Computer Weekly



## United States

- Authorized push payment fraud losses in the US are expected to reach over \$3 billion by 2026, doubling from 2021.<sup>6</sup>
- Zelle—a popular P2P payment service—was recently the subject of congressional scrutiny due to the scale of the scams.



*Overall, four banks that provided data reported over 190,000 cases ... involving over \$213 million of payments in 2021 and the first half of 2022. In the vast majority of these cases, the banks did not repay the customers that were defrauded. Overall the three banks that provided full data reported repaying customers in only 9.6% of scam claims, and repaid only \$2.9 million, representing 11% of payments.<sup>7</sup>*

Senator Elizabeth Warren



- It should be noted that this is only partial data drawn from only three banks. Zelle is owned by a conglomerate of some of the biggest US banks, but is connected to over 1,700.<sup>8</sup>
- Federal Trade Commission data shows that in 2022 alone about 1 in 5 people lost money to imposter scams—a whopping \$2.7 billion in losses with a \$1,000 median.<sup>9</sup> APP fraud played a part in more than \$1.6 billion of those.
- FedNow is coming to bring real-time payments as a standard across the US, but there are serious concerns as to whether institutions are ready for it. Initial feedback at industry events suggests that days-long transaction reviews may come back in force.
- A recent court ruling in *Studco v. 1st Advantage* could set a precedent for financial institutions hosting accounts that receive illicit funds.<sup>10</sup> These institutions would need to reimburse losses if their transaction monitoring systems generate alerts about discrepancies between the intended recipient and the fraudulent account owner.

<sup>6</sup> "APP fraud volumes expected to double by 2026, says report," *Computer Weekly*

<sup>7</sup> "New Report by Senator Warren: Zelle Facilitating Fraud, Based on Internal Data from Big Banks," Office of Senator Elizabeth Warren

<sup>8</sup> "Get Started With Zelle," Zelle

<sup>9</sup> "The Big View: All Sentinel Reports," Federal Trade Commission

<sup>10</sup> "Federal Court Holds Financial Institution Liable for Business Email Compromise Loss," Davis Wright Tremaine

## United Kingdom

- APP fraud represented **41% of all fraud losses** in the UK in the first half of 2022, just under £250 million.<sup>11</sup>
- The recently passed Financial Services and Markets Act will put pressure on all involved actors by making financial institutions liable for reimbursing APP fraud victims.<sup>12,13</sup> Starting in 2024, **the responsibility for customer reimbursement will fall on both the sending and receiving institutions.**
- There is a proposal to expand Confirmation of Payee measures that require payment services providers (PSPs) to collect additional information about the receiving account when both the sender and receiver are UK-based accounts.<sup>14</sup>
- The Financial Conduct Authority (FCA), in a widely read "Dear CEO" letter, singled out payment institutions (PIs) and other electronic money institutions (EMIs)—challenger and neobanks—for KYC and AML failures indicative of the risks from APP fraud.<sup>15</sup>



*Our work with firms over the past two years has identified material issues with financial crime systems and controls at PIs and EMIs. Common issues include:*

- *Failure to carry out and/or to evidence adequate KYC/due diligence.*

*We have seen evidence of elevated fraud rates in some PIs and EMIs...Common weaknesses we have seen include:*

- *Weaknesses in firms' anti-fraud systems and controls; and*
- *a high proportion of customer accounts being used to receive proceeds of fraud.*

*We expect you to take immediate action to protect your firm's customers against the risk of fraud and to ensure that your firm is not being used to receive the proceeds of fraud.*

**Financial Conduct Authority**

<sup>11</sup> "2022 Half Year Fraud Update," UK Finance and LexisNexis

<sup>12</sup> "Financial Services and Markets Act", 2023

<sup>13</sup> "APP scams," Payment Systems Regulator

<sup>14</sup> "Specific Direction 17 on expanding Confirmation of Payee," Payment Systems Regulator

<sup>15</sup> "Portfolio Letter: FCA priorities for payments firms," Financial Conduct Authority.

## European Union

- While data on APP fraud impacts in the EU is, so far, thin, the European Banking Authority and the European Payments Council have noted the unique challenges related to the nature of the single currency market: fraudsters exploit cross-border transactions to make it more difficult for authorities and institutions to cooperate in stopping the scams.<sup>16</sup>
- The large-scale deployment of Payment Services Directive 2 (PSD2) and 3D Secure (3DS) has helped curtail some of the impact of some other frauds through measures such as strong customer authentication. But since humans themselves are the weak point in instant payment scams, regulators have already noted that these directives have shortcomings—shortcomings that, unaddressed, could make APP fraud the path of least resistance, supercharging the technique.<sup>17</sup>

To address this, the European Commission in June 2023 announced that work is beginning on a PSD3 and an associated Payment Services Regulation.<sup>18</sup> Their proposal specifically notes fighting APP-like frauds and **implementing UK-like refund measures** as a primary goal:

**Combat and mitigate payment fraud**, by enabling payment service providers to share fraud-related information between themselves, increasing consumers' awareness, strengthening customer authentication rules, extending refund rights of consumers who fall victim to fraud and making a system for checking alignment of payees' IBAN numbers with their account names mandatory for all credit transfers.

European Commission

- Anecdotal evidence shows that problems arising from APP fraud are significant enough for many banks to bar consumers from making transfers to what they consider high-risk neobanks or payment institutions.

<sup>16</sup> "Discussion Paper on the payment fraud data received under PSD2 (EBA/DP/2022/01)—Submission #10," European Banking Authority.

<sup>17</sup> "2022 Payment Threats and Fraud Trends Report, Version 1.0," European Payments Council.

<sup>18</sup> "Modernising payment services and opening financial services data: new opportunities for consumers and businesses," European Commission.

## What recourse do victims have?

Unless they have been hacked or had their account information somehow compromised—usually via stolen devices or social engineering institutions' customer support departments—victims of APP fraud are generally considered to be the responsible party with full liability for the losses. Some banks in the US, for example, have argued that victims are "recruited" into becoming willing participants who personally authorize a transaction to avoid reimbursing customers. From this strictly legalistic point of view, the act of authorizing a payment can let institutions off the hook.

In practice, though, victims feeling abandoned by their financial institution in their moment of need can result in severe brand and reputational damage.<sup>19</sup> The media has been quick to capitalize on the stories of "big bad banks" leaving consumers in the cold.



*It's like the banks have colluded with the sleazebags on the street to be able to steal...I filed grievances with every agency I could get my hands on, locally and nationally. Every response I got was useless.*

**Bruce Barth, a victim of APP fraud**



But more significantly, consumers talk with their money—by walking:<sup>20</sup>

**72%**

of victims close their accounts after the fraud occurs

**13%**

do not open a new one with the same provider

This sort of customer flight is a much more frightening proposition for any financial institution. Given the choice of reimbursing the average \$1,000 loss, or losing all future earnings from that account and dealing with reputational fallout, most institutions choose to voluntarily reimburse 80% of the time.

But if regulations like those proposed in the UK become the international norm, the choice of reimbursing or not may soon be taken out of institutions' hands—meaning consumers will feel better, but financial services across the board will really start to feel the pinch.

<sup>19</sup> "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem.," [New York Times](#)

<sup>20</sup> "Scamscope: APP scam trends in US, UK, and India," [ACI Worldwide and GlobalData](#)



## SECTION 02

# WHAT'S DRIVING APP FRAUD

---

Newcomers are always easy to blame, but the challenges APP fraud poses to FRAML regimes is industry wide.

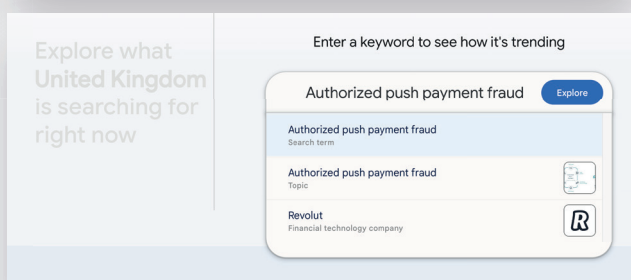
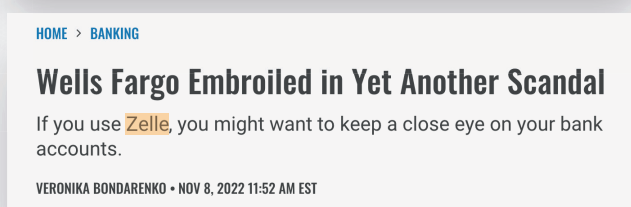
## Growth-focused business models under fire

A lot of fingers point at fintechs as being responsible for the sudden explosion in APP fraud. Leaving aside for now the validity of this argument and whether the industry recognizes any responsibility for the issue, the consequences of this booming fraud technique are already starting to pile up into a significant threat to any up-and-coming fintech.

## Reputation, trial by media, and the death of convenience

If fintechs are perceived by other financial institutions and players to be high risk, they will essentially be treated as pariahs by the rest of the financial system. Not only will regulators be unwilling to fight back on their behalf, this means fintechs will eventually be cut off from the system altogether. **Fintechs deemed "high risk" will be unable to transact.**

In fact, high-profile media outlets have already covered numerous examples of this exact chain of events.



*Trial by media is an expression of the reputational damage that can negatively affect trust and customer acquisition before the services get cut off altogether.*

- Robinhood has refused to receive incoming funds from a series of fintechs and their banking backers.<sup>21</sup>



*"LendingClub; Ohio-based Sutton Bank (one of the partner banks that Square's Cash App uses to store customer deposits); Tennessee-based First Century Bank (one of the partner banks for PayPal's Cash Card); prepaid card issuer and digital bank Green Dot; New York-based Metropolitan Commercial Bank (the partner bank for digital bank Current); and Iowa-based Lincoln Savings Bank (one of the partner banks for fintech apps such as Cash App and Acorns). Pittsburgh-based PNC Bank—the nation's seventh largest bank by assets—and its recent acquisition BBVA USA are also on Robinhood's banned list, Forbes has been told.*

**from "With Fraud Growing, Robinhood Becomes Latest Fintech To Block Customers From Transferring Money From Certain Banks" in Forbes**



- Chime, Green Dot, Cash App, and, ironically, Robinhood itself—along with other prominent payment fintechs—have been blacklisted by financial services and point-of-sale users ranging from rental car outlets and liquor stores<sup>22</sup>



*Budget would not accept [Robyn Mathis's] Chime credit or debit card. Frustrated, Mathis, who was traveling with her two college-aged children, called other airport rental outlets—Enterprise, Avis, and Dollar. All said they wouldn't take her card. After two hours, Mathis finally gave up and called an Uber. Fintech had failed her.*

**from "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards" in Forbes**



*Betterment, a robo-investing app with \$29 billion in assets, blocked all new connections to Chime, Cash App, Square, Robinhood, Green Dot, and Metabank.*

**from "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards" in Forbes**



<sup>21</sup> "With Fraud Growing, Robinhood Becomes Latest Fintech To Block Customers From Transferring Money From Certain Banks," Forbes

<sup>22</sup> "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards," Forbes

This is a two-pronged existential problem for all payment firms and neobanks.

- 01 **Threat to convenience:** Convenience is the key fintech value proposition for acquiring customers. Even though around 8 in 10 North Americans have linked their main bank accounts to a fintech service, only 14% claim to trust fintechs.<sup>23</sup> If customers cannot use the service, they will go elsewhere. To continue Mathis's experience above:

80%

linked main bank  
accounts to a fintech  
service

14%

claim to trust  
fintechs



*Upon returning home, she moved most of her money from Chime to her account at Bank OZK, a regional institution with more than 200 branches and roots stretching back to 1903.<sup>24</sup>*

**from "With Fraud Growing, Robinhood Becomes Latest Fintech To Block Customers From Transferring Money From Certain Banks" in Forbes**



- 02 **A reason to be smothered by incumbents:** Traditional banks clearly recognize that new up-and-comers are a threat thanks to business models that focus squarely on winning over customers with convenience and lower fees.<sup>25</sup> Becoming a high-risk counterparty is the perfect excuse to nip their competitors' growth in the bud.

<sup>23</sup> ["The rise of open banking," Mastercard](#)

<sup>24</sup> ["Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards," Forbes](#)

<sup>25</sup> ["Fintechs Are Taking A Bite Out Of Banks: What This Means For Businesses," Forbes](#)

## Greater regulatory scrutiny & mandatory reimbursements

Across all major markets, regulators are starting to take a closer look at fintechs that, while perhaps not systemically important in the strictest sense of the term, carry such weight in specific jurisdictions or sectors that the entire financial system may feel knock-on effects from risks and disruptions among these newcomers.

This increased attention started a few years ago with crypto and the impact of buy now, pay later (BNPL) services on consumer debt, but has now shifted to the challenges posed by APP fraud in the context of real-time payment systems. Neither the FCA's "Dear CEO" letter of early 2023 nor the US Senate's inquiry into Zelle minced words regarding the KYC and AML failings of payment firms and neobanks:



*We expect you to take immediate action to protect your firm's customers against the risk of fraud and to ensure that your firm is not being used to receive the proceeds of fraud.*

**Matthew Long, Director, Payments & Digital Assets on behalf of the FCA**



While it remains to be seen just how aggressive regulators' follow-up actions will actually be, it's well within the realm of possibility that non-fulfillment of new compliance requirements could result in freezes on activities such as further customer acquisition, new product launches, or entries into new markets until such time as the institution is compliant. These are all factors that could starve a startup of growth—accelerating its burn rate and curbing interest among new investors.

Most worrisome of all, however, is the likelihood for regulatory mandates to follow the British lead of spreading reimbursement responsibilities between both institutions involved in an APP scam transaction—that is, requiring both the institution that hosts the victim account as well as the institution hosting the fraudster's receiving account to pay up. We are already seeing hints of this in the EU's initial PSD3 proposals. On one hand, victim accounts can easily come from anywhere in the financial ecosystem, meaning industry-wide interest in cutting out APP fraud wherever it crops up—and further grinding the axe with respect to any institution seen to be abetting the issue.

On the other hand, as we'll see in a moment, APP fraudsters need a significant number of money mules to keep their scam going. The risk of proliferating mule accounts is likely to be concentrated in institutions that offer (or prioritize) remote onboarding experiences.

# Are fintechs truly more exposed?

---

Obviously the fintech industry is the current subject of ire from the media, regulators, and traditional competitors alike. But is this even justified? Are fintechs truly more vulnerable to APP fraud? For an accurate answer, we first need to map out the mechanics of the fraud and how they interact with the particularities of fintechs.

## Anatomy of APP fraud

APP fraud can be broken down into 3 parts:



### THE SCAM

---



### THE MULE

---



### THE TRAILBREAKER

## The Scam

As mentioned before, APP fraud is usually a component of broader scams. Most of these are variations on the **Imposter** or **Impersonation scam**, where a scammer impersonates someone the victim knows—a friend, family member, or even a company they do business with—and requests an urgent or unexpected payment.

These requests can come through any channel: email, SMS, chat, or more. There have even been cases of spear phishing attacks using deepfakes of CEOs or other executives to fool victims over the phone.<sup>27</sup> And with the growing accessibility of generative AI, the options will only grow.<sup>28</sup>

Whatever the method, there is usually one of two end results:

- The victim changes the destination and/or amount of a standing transaction order on their account, or
- The victim creates and authorizes a new one-off payment.

### Favorite APP fraud starting points

#### Purchase scam

A fraudster advertises a product online and convinces the victim to pay via bank transfer, after which the fraudster disappears without providing the product.

#### Rental scams

Scammers pose as landlords or property agents and ask for deposits or rent payments upfront, but the property isn't actually available for rent or doesn't exist at all.<sup>26</sup>

#### Invoice redirection fraud and business email compromise (BEC)

A scammer poses as a legitimate supplier and provides the victim with fraudulent bank details for payment, causing the victim to send money to the criminal's account instead of the actual supplier.

#### CEO fraud

Fraudsters target businesses by impersonating a high-ranking executive or business partner requesting urgent payments or transfers to their bank account.

#### Romance scams, a.k.a. pig butchering

Fraudsters develop online relationships with victims and convince them to send money for various reasons, such as medical emergencies or travel expenses.

#### Investment scam

Scammers lure individuals or businesses into making financial investments with false promises of high returns.

<sup>26</sup> "Vacation rental scam: Valley home listed on rental site without owners' knowledge," KNXV and Scripps Media

<sup>27</sup> "AI-generated voice deepfakes see growing use in cyberattacks," Protocol

<sup>28</sup> "FraudGPT: How AI is—and isn't—revolutionizing financial crime," Resistant AI

## The Mules

For obvious reasons, the account where the fraudster first receives the proceeds of a social engineering scam can't be the final destination: it would be very easy to find and retrieve the funds if that were the case. Savvy fraudsters will instead need multiple mule accounts for two reasons:

- 01 **Backing up their receiving accounts:** Unless skilled fraudsters are spear phishing for abnormally large one-off payments, they will be operating their scams at a relatively industrial level, blasting a lot of potential targets for relatively small sums, with volume making up the difference. With their "marketing" campaign generating fresh leads, they'll need backup accounts waiting in the wings if—or when—their main receiving mule is taken down.
- 02 **Building a laundering network:** They'll also need a contingent of other accounts to forward the money to. This is not so much to layer the proceeds in preparation for integration,<sup>29</sup> since the source of the funds will be uncovered as a scam and any related account will be suspect. Instead, fraudsters will use the same instant payment infrastructure that kicked off their scheme to cover—or at least complicate—their tracks, buying time to prepare for the final phase of the scam: getting the money to an exit account and breaking the money trail.

It's important to elaborate on this second point in no uncertain terms. The account that receives fraudulent funds from the victim is only the first in a string of money mule accounts.

**With every "hop" from mule to mule, the inciting act of fraud merges with AML compliance: the funds are now being laundered.**

Of the different types of mules, only synthetic money mules offer the scale and control needed to execute these scams properly.

---

<sup>29</sup> A reminder on the three stages of money laundering: placement—getting the money in; layering—distancing the money from the source; integration—legitimizing the proceeds.

## Why APP fraud thrives on synthetic money mules

Just as APP fraudsters use a variety of techniques to start their scams, gaining control of money mules can take many forms: account takeovers, coercion, even well-paid willing participants.<sup>30</sup> But synthetic money mules are in a league of their own—one perfectly suited to the digital nature of APP fraud.

### Low cost

Synthetic money mule accounts are created using a mix of real, stolen, and/or forged documentation. With personal information easily obtainable on the (dark) web, document templates discoverable with just a web search, image editors free for download, and now generative AI, it's possible for anyone, anywhere to assemble enough convincing personal data to successfully fool unprepared KYC processes—no need for painstaking paper or plastic fakes.

### Low risk

Digital onboarding then turns the security standoff between banks and fraudsters into an iterative game. Instead of only a few attempts to create fraudulent accounts in the physical world, attackers in the digital realm operating out of potentially unassailable jurisdictions get an essentially unlimited number of attempts to probe target systems. So while repeated in-person attempts risk arrest every time, digital criminals incrementally learn from the explicit and side-channel feedback they glean over hundreds of attempts—with essentially no personal risk.

The kicker is that if, or more likely when, a mule account is found out, there's no one for authorities to come down on: the account was fake from start to finish, and fraudsters can just disappear into another synthetic identity.

### High scalability

Once attackers identify even minor gaps in their target's digital systems, digital means can also exploit them exponentially. For instance, knowing how to fake documents that bypass security checks opens the door to industrial-scale forgeries. Or bots may be trained to automatically navigate onboarding processes over and over again.

In the end, taking the synthetic route gives digital fraudsters direct access to a nearly unlimited number of money mule accounts.

<sup>30</sup> ["The Rise of Money Launderers on Snapchat and Instagram", Vice Media](#)

## The Trailbreaker

Once fraudulent proceeds have moved through the financial system and have been distanced from the initial receiving account, criminals need a way to break the trail, a way to get the money out of the financial system as quickly as possible.

But why break the trail? Why not just integrate the proceeds?

Simply put, breaking the trail adds an additional level of security and deniability. Since any account the money flows through becomes an accessory to the (at this point numerous) crimes, if the proceeds were integrated into a single account at the end of the trail, successful investigations could uncover the whole pot.<sup>31</sup> Instead, successful APP schemes extract the proceeds from the preceding string of fraud and money laundering by converting digitally moved funds into cash, crypto, or goods.

Once proceeds have been extracted and the trail broken, the likelihood of recovering scammed funds nosedives, and fraudsters can abandon their money mule networks—after all, they've used them for their purpose and they can just make more if they want another go-round. It's key, then, to tackle the issue before it gets to this point.

### Popular exit routes

#### Cryptocurrencies

Crypto is an effective, if complex, way to break with the traditional financial system. Fraudsters convert their earnings to crypto, transfer the crypto to a private wallet, convert it to other crypto on a decentralized exchange, use a crypto tumbler as an automatic laundering operation, or a combination of the above. The laundered funds are usually converted back into fiat.

#### Cash mules

Nothing beats cold hard cash, and criminals often rely on real-life money mules—people they've coerced or professional mules—to get it. Drug gangs are even known to advertise on social media how much money can be made this way: mules are paid promptly in cash and simply report to police that their phones and identities were stolen.

#### Fake purchases

Trailbreaker mules don't need to be people. By making "purchases" from a front business—which may or may not have actual merchandise or services to sell—the trail of money is obscured by having clear payment orders.

#### Real purchases

Other times you want the real deal. Big, illiquid assets such as houses can be liabilities, but smaller high-value items, often with high resale value, can effectively remove money from the system. Examples are luxury items from cars to electronics; non-fungible tokens (NFTs), which combine purchases and crypto without dealing with physical objects; or even financial instruments like options trading or crypto derivatives.

<sup>31</sup> The exception always exists, of course. Criminals who have access to a broad inter-company or international set of money mule accounts can significantly hinder investigations. But the risk is always there that after some time the final integration point is discovered, so the smart move is to cover their tracks by breaking off the trail.

# Are fintechs truly more at risk?

---

With rapid money movement and abundant money mules as clear cornerstones for successful APP scams, fintechs still seem to be a welcoming ecosystem for a variety of reasons.

## Speed facilitates APP fraud

Digital-only banks and payment firms have long distinguished themselves by offering proprietary payment mechanisms which offer near real-time or immediate transfer mechanisms—particularly amongst their own users. But speed is also crucial to keeping the money moving before suspicion is acted upon and transactions frozen.

But in response, traditional institutions have created their own fast payment rails—TCH Real-Time Payments (RTP), Faster Payment Services (FPS), Zelle, and others—which will open them up to similar issues soon.

## Exploiting digital-only convenience

Many payment firms and fintechs have streamlined their operations around digital-only or -first experiences. But fraudsters too can benefit from the ability to open accounts 24/7 without ever coming face to face with another human being, potentially even from another jurisdiction.

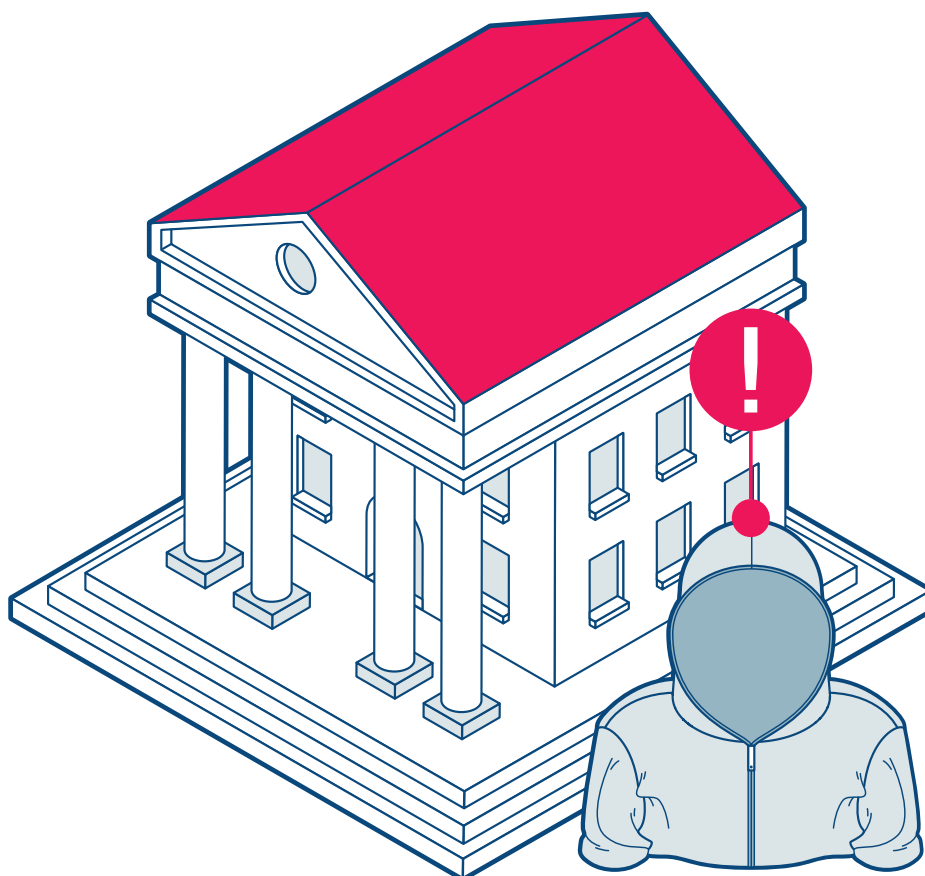
What's more, fraudsters can leverage this completely online process: using false identities, automation tools, and support groups like any other online community, fraudsters can and do exploit digital-only processes time and time again to stand up their armies of money mule accounts. Behind a computer screen, the risk of being apprehended for attempted fraud is near zero, while the number of potential money mule accounts is near limitless.

Meanwhile, financial services with non-digital—or at least slower and clunkier—digital onboarding experiences actually make it more difficult for criminals to create the mule accounts they need. **Ironically, having great digital UX and well-maintained and documented APIs makes you a bigger target.**

## Growth as an achilles heel

Payment firms and neobanks also often hang their hat on rapid growth—and why not, since it's a mark of success, a free marketing tool, and attractive to investors. But there's a more pernicious effect of rapid growth too: fraud tends to be more concentrated in new accounts. The longer an account is in existence, more likely it is legitimate and the less likely it is to be used to commit a crime.

Therefore, fast-growing payment firms will, by their nature, hold a higher proportion of fraudulent accounts compared to older institutions with slower growth and more established customer bases simply by nature of the age distribution of the accounts.<sup>32</sup>






<sup>32</sup> "When is a bank account not a bank account?," Alloy

## Banks, neobanks, and statistics: Traditional banks fare no better than fintechs

But taking a close look at hard numbers is where the misapprehension of risky fintechs begins to unravel.

In the spring of 2023, *The Sunday Times* published an exposé comparing fraud-related account freezes in neobanks and traditional institutions.<sup>33</sup> They suggested that a disproportionate amount of such fraudulent accounts are held by neobanks—who held 25% of frozen accounts despite enjoying only an 8% market share—and that there is a three- to seven-fold difference in fraudulent assets when normalized against the entire customer base.

### APP-related accounts frozen under Section 303Z1 of the 2002 Proceeds of Crime Act

	Company	Freeze orders	Amount frozen	Money frozen per customer
●	 <b>wise</b>	86	£11,494,649	£0.72
●	<b>tide</b>	13	£548,620	£1.10
●	<b>Revolut</b>	78	£2,645,417	£0.44
●	 <b>monzo</b>	13	£1,289,250	£0.18
●	 <b>BARCLAYS</b>	62	£4,019,705	£0.17
●	<b>LLOYD'S</b>	78	£3,029,319	£0.11

Source: Sunday Times analysis of Courtsdesk data, October 2022-April 2023

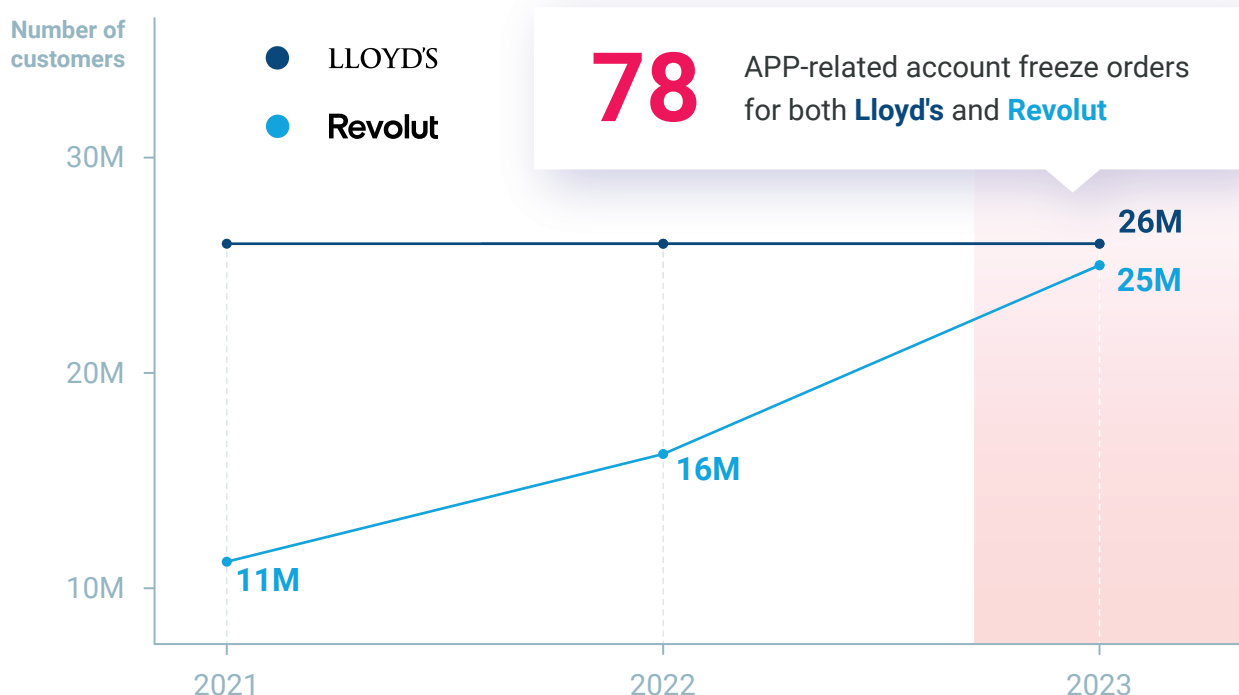
● Neobank

● Traditional bank

<sup>33</sup> ["Why do fraudsters seem to love the new breed of bank?" The Sunday Times](#)

But as with any statistics, averages only give you part of the story. The damning revelation is that the number of frozen accounts across the different institutions in the report—both new and old—are all in the same range. This is even as older institutions had far fewer account openings over that time: **Lloyd's customer base, for example, stayed flat at 26 million between 2021<sup>34</sup> and 2022<sup>35</sup> while Revolut added 9 million users in 2022 alone.<sup>36</sup>** There is not, in fact, less fraud among established players: the larger denominator—their larger number of total accounts—merely creates the illusion they are better insulated against it.

Working from the premise that incumbent banks are onboarding far fewer customers—and fewer still through digital-only channels—the comparative numbers indicate that the appearance of inordinate fraud challenges isn't a result of fintechs' business models or willingness to turn a blind eye, but rather a result of even the slightest gaps in one of the things that makes them most unique: their digital onboarding and KYC processes.



<sup>34</sup> "Lloyds Banking Group Annual Report and Accounts 2021," Lloyds Banking Group

<sup>35</sup> "Lloyds Banking Group Annual Report and Accounts 2022," Lloyds Banking Group

<sup>36</sup> "Revolut posts over £100m adjusted EBITDA with £26.3m profit in first full year of profitability," Revolut



## SECTION 03

# WHY—AND HOW—FINTECHS MUST LEAD THE FIGHT

---

Pioneers of digital approaches to banking can also blaze the trail when it comes to digital fraud countermeasures.

## Fintechs are where the solution starts

---

As we've laid out above, fintechs don't see anything other than their share of fraud—and they certainly don't welcome it. And as financial services, including established players, continue to digitize, any organization employing a digital-first or -only approach will be hit by attackers probing for easy places to stand up their money mules.

So it may seem somewhat contradictory to propose that fintechs take the lead on tackling the issue of APP fraud. **But it's precisely because neobanks and fintechs have innovated convenient, low-friction digital onboardings that they are best suited to employ the most sophisticated technological countermeasures.**

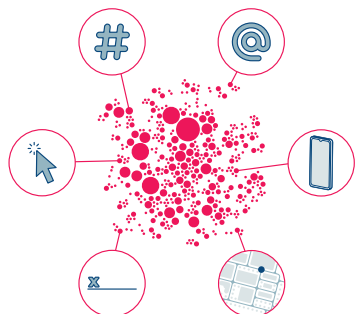
### The friction-free way to cut out APP fraud from your user base

The real risk today is relatively minor gaps in digital KYC onboarding processes. Synthetic fraudulent identities and scalable attacks work together to exploit these gaps in the form of easy-to-create money mule accounts disproportionately concentrated within neobanks that are pioneers in digital services.

So it might seem reasonable to require digital banks to increase the friction and selectivity of their KYC process by several orders of magnitude just to keep their risks at an acceptable level. This is not so: instead of increasing friction, existing data can be used to address scalable risks far more effectively.

This is exactly the game we play on behalf of our customers. The job of Resistant AI is to reliably defy scalable attacks using machine learning techniques that outsmart criminals' technology. To do so, we don't rely on silver bullets: in the real world, no technology is bulletproof. Instead, we rely on scientifically designed interlocking defenses, where multiple independent layers progressively reduce the level of threat and cover each other's blind spots.

## The Resistant AI approach: Defense in depth



### Preventing mules before onboarding

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



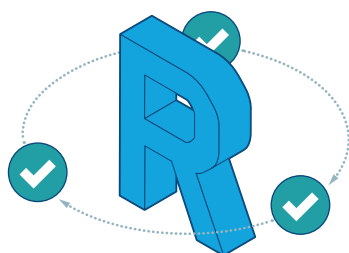
### Preventing mules during onboarding

You intake customer documents as normal, and Document Forensics automatically analyzes them for forgeries and serial fraud. Not only does this uncover digital alterations that fool traditional checks, it blocks patterns of reused documents like forgery templates and stolen identities. This helps eliminate up to 90% of manual reviews, though our 99.2% accuracy rate effectively prevents the creation of new fraudulent money mule accounts altogether.



### Clean out accounts connected by transactions

In real time, Transaction Forensics allows you to identify behaviors consistent with the movement of fraudulent funds among money mule networks. Specially developed detectors use statistical anomalies to flag suspicious money flow typologies and relationships between accounts—relationships that point to fraudulent accounts, account takeovers, and other bad actors.



### Apply learning for perpetual KYC

The information our combined products glean throughout the preceding steps is applied recursively to the rest of your network. Documents revealed to be forged or stolen may weed out accounts previously thought to be legitimate, while scams in progress or sleeper agents may be uncovered if customers deviate from their normal behaviors.

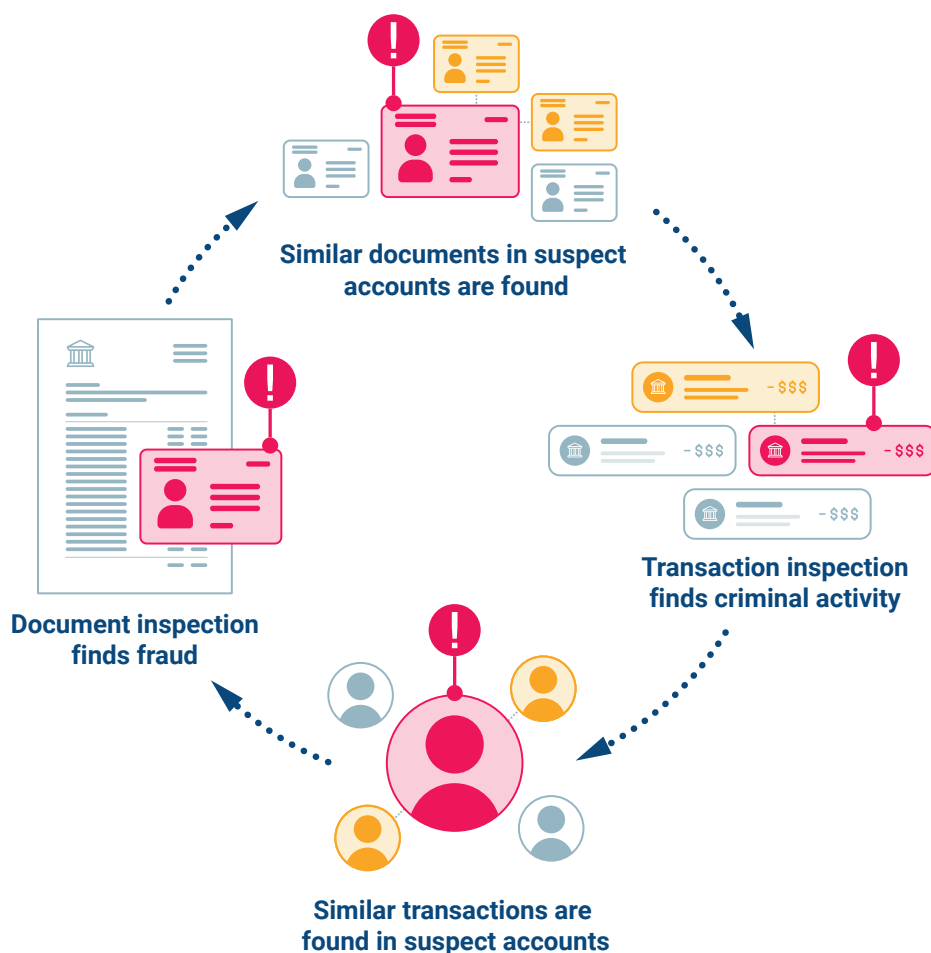
## Why a layered approach works

Combining insights from customer documentation, identities, behaviors, and transactions—for both new and existing customers—prevents the creation and scaling of synthetic money mule accounts. In so doing, it returns the initiative to financial institutions.

By spreading out detections over the entire customer life cycle, criminals can never be certain whether their accounts have already been detected as potential money muling accounts or will be very soon. In turn, this uncertainty reduces their accounts' resale value on the black market: no APP gang wants to transfer stolen cash through accounts that are likely to be blocked the moment fraudulent proceeds reach them.

The ability to effectively stop the proceeds of APP fraud is a strong deterrent for subsequent attackers. As soon as they start losing money, they will use sleeper mules in other banks.

That's why preventing the creation and use of money mule accounts that move fraud proceeds and then extract them from the financial system is the only effective way to reduce APP fraud. It breaks the criminal business model, protects institutions from reimbursement charges, and preserves the low-friction financial services ecosystem we are building as an industry.



## Steps any organization can take now

---

### Audit your customer base to determine your exposure

Any organization with digital onboarding is at risk from this threat—and most likely already has some exposure. The question is how large. Running an audit is an easy first step that will give you the information you need to understand how seriously your business is impacted.

### Start layering AI into your tech stack now

Existing rules-based systems and rigid automated onboarding workflows are often siloed and incapable of dealing with the complexity of the challenge posed by constantly evolving criminal behaviors, while replacing your existing tech stack to take advantage of AI is costly both financially and operationally, and takes time you can't afford to lose.

But you don't have to wait. At its heart, machine learning is a decisioning mechanism that can and should be layered into your existing tech stack to help you start the transition.

**Resistant AI can help you with both of these.**

**To get in touch, please reach out to us at [resistant.ai](https://resistant.ai)**



## Joe Lemonnier

Head of Product Marketing, Resistant AI

*Joe has been digging into the intersections of tech and criminality for over 10 years, and brings a wealth of experience in customer research, design, product strategy and development, and content and thought-leadership to Resistant AI. His skills were honed in cybersecurity, online privacy, and productivity services that met the needs of hundreds of millions of users, and he's helped to drive business growth through service expansions and revamps, new-product discoveries and launches, and portfolio streamlinings. Engaging with customers to define seamless protective solutions are the main things that get him up in the morning.*

 [www.linkedin.com/in/jklemonnier/](https://www.linkedin.com/in/jklemonnier/)

 [Joe.Lemonnier+bio@resistant.ai](mailto:Joe.Lemonnier+bio@resistant.ai)

- 1 Phil Muncaster, "Authorized Push Payment Surges to 75% of Banking Fraud," Infosecurity Magazine, last updated 22 September 2022, <https://www.infosecurity-magazine.com/news/authorized-push-payments-75/>.
- 2 "Discussion Paper on the payment fraud data received under PSD2 (EBA/DP/2022/01)—Submission #10," European Banking Authority, accessed 30 May 2023, <https://www.eba.europa.eu/node/107695/submission/125221>.
- 3 Lucas Mearian, "Fed's Zelle-like instant payment system to go live in July, hundreds now testing," Computerworld, 17 April 2023, <https://www.computerworld.com/article/3693256/fed-s-zelle-like-instant-payment-system-to-go-live-in-july-hundreds-now-testing.html>.
- 4 Muncaster, "Authorized Push Payment Surges."
- 5 Alex Scroxtion, "APP fraud volumes expected to double by 2026, says report," Computer Weekly, 15 November 2022, <https://www.computerweekly.com/news/252527286/APP-fraud-volumes-expected-to-double-by-2026-says-report>.
- 6 Scroxtion, "APP fraud volumes."
- 7 "New Report by Senator Warren: Zelle Facilitating Fraud, Based on Internal Data from Big Banks," Office of Senator Elizabeth Warren, 3 October 2022, <https://www.warren.senate.gov/oversight/reports/new-report-by-senator-warren-zelle-facilitating-fraud-based-on-internal-data-from-big-banks>.
- 8 "Get Started With Zelle," Zelle, accessed 30 May 2023, <https://www.zellepay.com/get-started>.
- 9 "The Big View: All Sentinel Reports," Federal Trade Commission, last updated 25 April 2023, <https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports>.
- 10 "Federal Court Holds Financial Institution Liable for Business Email Compromise Loss," Davis Wright Tremaine, 24 February 2023, <https://www.dwt.com/blogs/privacy-security-law-blog/2023/02/business-email-compromise-bec-studco-1st-advantage>.
- 11 "2022 Half Year Fraud Update," UK Finance and LexisNexis, accessed 30 May 2023, <https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf>.
- 12 Financial Services and Markets Act, 2023, c. 1, [https://www.legislation.gov.uk/ukpga/2023/29/pdfs/ukpga\\_20230029\\_en.pdf](https://www.legislation.gov.uk/ukpga/2023/29/pdfs/ukpga_20230029_en.pdf).
- 13 "APP scams," Payment Systems Regulator, accessed 15 June 2023, <https://www.psr.org.uk/our-work/app-scams/>.
- 14 "Specific Direction 17 on expanding Confirmation of Payee," Payment Systems Regulator, 24 October 2022, <https://www.psr.org.uk/media/zxgkagpj/psr-specific-direction-17-expanding-confirmation-of-payee-oct-2022.pdf>.
- 15 Matthew Long, "Portfolio Letter: FCA priorities for payments firms," Financial Conduct Authority, 16 March 2023, <https://www.fca.org.uk/publication/correspondence/priorities-payments-firms-portfolio-letter-2023.pdf>.
- 16 European Banking Authority, "Discussion Paper." <https://www.eba.europa.eu/node/107695/submission/125221>.
- 17 "2022 Payment Threats and Fraud Trends Report, Version 1.0," European Payments Council, 23 November 2021, <https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf>.
- 18 "Modernising payment services and opening financial services data: new opportunities for consumers and businesses," European Commission, 28 June 2023, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_3543](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543).
- 19 Stacy Cowley and Lananh Nguyen, "Fraud Is Flourishing on Zelle. The Banks Say It's Not Their Problem.," New York Times online, 6 March 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

- 20 "Scamscope: APP scam trends in US, UK, and India," ACI Worldwide and GlobalData, accessed 30 May 2022, <https://drive.google.com/file/d/1sC7OCB12WKxmxHUcb5-ukSMcsaPvBqUu/view>.
- 21 Jeff Kauflin and Eliza Haverstock, "With Fraud Growing, Robinhood Becomes Latest Fintech To Block Customers From Transferring Money From Certain Banks," Forbes online, 20 December 2021, <https://www.forbes.com/sites/jeffkauflin/2021/12/20/with-fraud-growing-robinhood-becomes-latest-fintech-to-block-customers-from-transferring-money-from-certain-banks/>.
- 22 Eliza Haverstock and Jeff Kauflin, "Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards," Forbes online, 3 December 2021, <https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=4dfe10a975bd>.
- 23 "The rise of open banking," Mastercard International Incorporated, accessed 30 May 2023, <https://drive.google.com/file/d/10HoRcG3R2Sg6dWHtWkEkM1qso8MvHlyG/view>.
- 24 Haverstock and Kauflin, "Fintech's Fraud Problem."
- 25 Greg Cohen, "Fintechs Are Taking A Bite Out Of Banks: What This Means For Businesses," Forbes online, 10 May 2022, <https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/10/fintechs-are-taking-a-bite-out-of-banks-what-this-means-for-businesses/>.
- 26 Joe Ducey, "Vacation rental scam: Valley home listed on rental site without owners' knowledge," KNXV and Scripps Media, last updated 19 May 2021, <https://www.abc15.com/news/let-joe-know/vacation-rental-scam-valley-home-listed-on-rental-site-without-owners-knowledge>.
- 27 Kyle Alspach, "AI-generated voice deepfakes see growing use in cyberattacks," Protocol, 18 August 2022, <https://www.protocol.com/enterprise/deepfake-voice-cyberattack-ai-audio>.
- 28 "FraudGPT: How AI is—and isn't—revolutionizing financial crime," Resistant AI, 19 April 2023, <https://resistant.ai/blog/fraudgpt-how-ai-is-revolutionizing-financial-crime>.
- 29 A reminder on the three stages of money laundering: placement—getting the money in; layering—distancing the money from the source; integration—legitimizing the proceeds.
- 30 "The Rise of Money Launderers on Snapchat and Instagram", Vice Media, 25 October 2021, [https://video.vice.com/en\\_uk/video/vice-the-rise-of-money-launderers-on-snapchat-and-instagram/6141d1cddb9b1767a411a791](https://video.vice.com/en_uk/video/vice-the-rise-of-money-launderers-on-snapchat-and-instagram/6141d1cddb9b1767a411a791).
- 31 The exception always exists, of course. Criminals who have access to a broad inter-company or international set of money mule accounts can significantly hinder investigations. But the risk is always there that after some time the final integration point is discovered, so the smart move is to cover their tracks by breaking off the trail.
- 32 Tommy Nicholas, "When is a bank account not a bank account?," Alloy, 20 December 2021, <https://www.alloy.com/blog/when-is-a-bank-account-not-a-bank-account>.
- 33 Ali Hussain and George Nixon, "Why do fraudsters seem to love the new breed of bank?," The Sunday Times, 23 April 2023, <https://www.thetimes.co.uk/article/why-do-fraudsters-seem-to-love-the-new-breed-of-bank-bbnkgg25g>.
- 34 "Lloyds Banking Group Annual Report and Accounts 2021," Lloyds Banking Group, 23 February 2022, <https://www.lloydsbankinggroup.com/assets/pdfs/investors/financial-performance/lloyds-banking-group-plc/2021/q4/2021-lbg-annual-report.pdf>.
- 35 "Lloyds Banking Group Annual Report and Accounts 2022," Lloyds Banking Group, 21 February 2023, <https://www.lloydsbankinggroup.com/assets/pdfs/investors/financial-performance/lloyds-banking-group-plc/2022/full-year/2022-lbg-annual-report.pdf>.
- 36 "Revolut posts over £100m adjusted EBITDA with £26.3m profit in first full year of profitability," Revolut, 1 March 2023, [https://www.revolut.com/en-CZ/news/revolut\\_posts\\_over\\_100m\\_adjusted\\_ebitda\\_with\\_26\\_3m\\_profit\\_in\\_first\\_full\\_year\\_of\\_profitability/](https://www.revolut.com/en-CZ/news/revolut_posts_over_100m_adjusted_ebitda_with_26_3m_profit_in_first_full_year_of_profitability/).

# resistant<sup>x</sup>ai



[www.resistant.ai](http://www.resistant.ai)

Credo.



Index Ventures

Seedcamp

NOTION