Fingerprint

# Scaling Trust in Digital Finance

Neobanks, BNPL,
and fraud in 2026

# Contents


| | |
|---|---|
| Executive Summary | 3 |
| Neobanks are now mainstream | 4 |
| Scale and speed have reshaped the fraud surface | 8 |
| Why onboarding concentrates risk earlier than teams expect | 9 |
| How AI and automation industrialize early-stage abuse | 11 |
| Scams now drive fraud outcomes, not just transactions | 13 |
| Authorized push payment (APP) fraud puts trust under a microscope | 15 |
| Account takeover and mule networks move faster at scale | 17 |
| When fraud becomes a compliance constraint | 19 |
| The growth vs. friction dilemma neobanks can’t avoid | 22 |
| What conversion-safe fraud prevention actually requires | 24 |
| How device intelligence supports trust at scale | 25 |
| Key takeaways | 27 |

## Executive Summary

Neobanks and digital lenders now sit at the center of customers' financial lives.

As more consumers rely on them as their primary financial provider, expectations around trust, reliability, and risk management have risen.

Fraud has evolved alongside scale. Coordinated, AI-enabled activity increasingly targets onboarding, messaging, installment lending, and early account activity, exploiting the speed of real-time payments and low-friction design.

Legacy fraud solutions struggle under these conditions. Controls built for slower, account-centric environments generate noise and friction without reliably stopping abuse across interconnected products.

Growth, lending, and risk are now tightly linked. Efforts to reduce fraud by adding friction can undermine experience and retention, while missed fraudulent activity increases financial and regulatory exposure.

Maintaining trust requires continuity, not checkpoints. Institutions that succeed in 2026 will invest in persistent signals and cross-journey visibility to manage risk without slowing down legitimate users.

> Neobanks didn’t just grow. They became primary financial institutions.

Over the past few years, neobanks (digital-first financial institutions that operate without physical branches) have shifted from secondary tools to central financial platforms. Customers increasingly rely on them to hold balances, move money, access credit, and manage everyday financial activity.

This evolution extends beyond neobanks alone. Buy now, pay later (BNPL) providers and other embedded finance models now operate alongside digital-first banks, expanding what “everyday finance” looks like inside a single application. Lending, installment payments, investing, and real-time transfers increasingly coexist within tightly integrated digital ecosystems.

As digital platforms take on a more central role in customers’ financial lives, the nature of risk changes with it. Trust is no longer established at a single moment. It now needs to persist across identity verification, onboarding, lending decisions, payment flows, and compliance obligations, often in environments defined by instant access and minimal friction.

This report examines how fraud in digital-first banking and BNPL environments has evolved in 2026, where pressure builds first, and what it takes to scale trust without sacrificing speed or customer experience.



## Neobanks are now mainstream

For much of the past decade, neobanks were defined by growth. Success was measured in app downloads, new account openings, and rapid user acquisition. Low-friction onboarding made it easy for customers to sign up, but many treated these accounts as secondary.

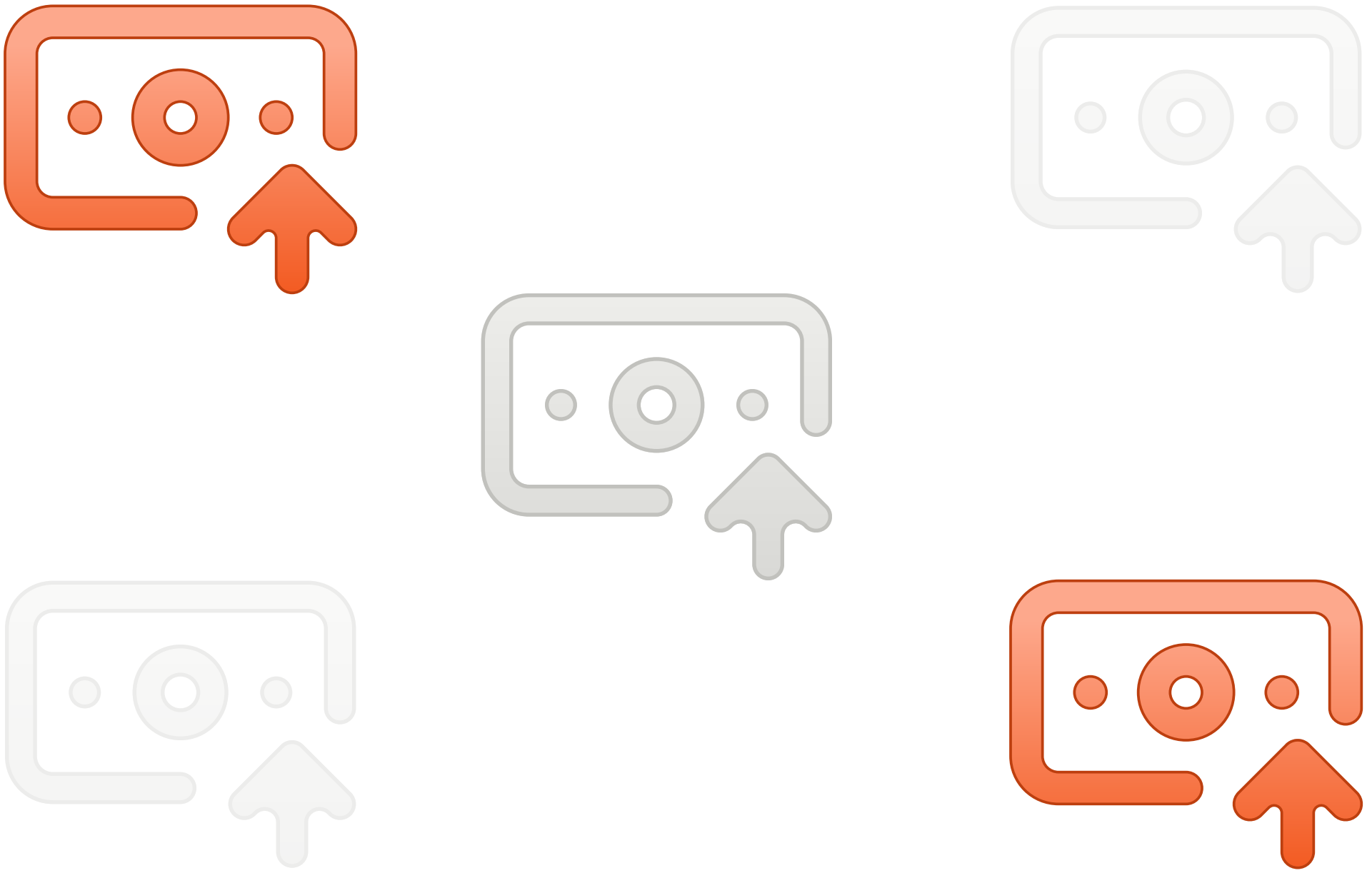
That dynamic has shifted.

### From secondary to primary relationships

More customers now rely on neobanks as their main banking relationship. In the U.S., neobanks' share of core banking relationships nearly doubled from 4.6% in 2022 to 8.7% in 2024. In the UK, that figure rose from 3.5% in 2022 to 5.9% by mid-2025. Nearly one in three U.S. consumers now considers a neobank their primary financial provider, particularly among users in their 30s.

In 2024 alone, neobanks captured nearly 44% of all new checking accounts opened, underscoring their shift from secondary tools to everyday financial platforms.

This move from experimentation to everyday use brings higher expectations around reliability, availability, and trust — expectations that more closely resemble those placed on traditional banks.



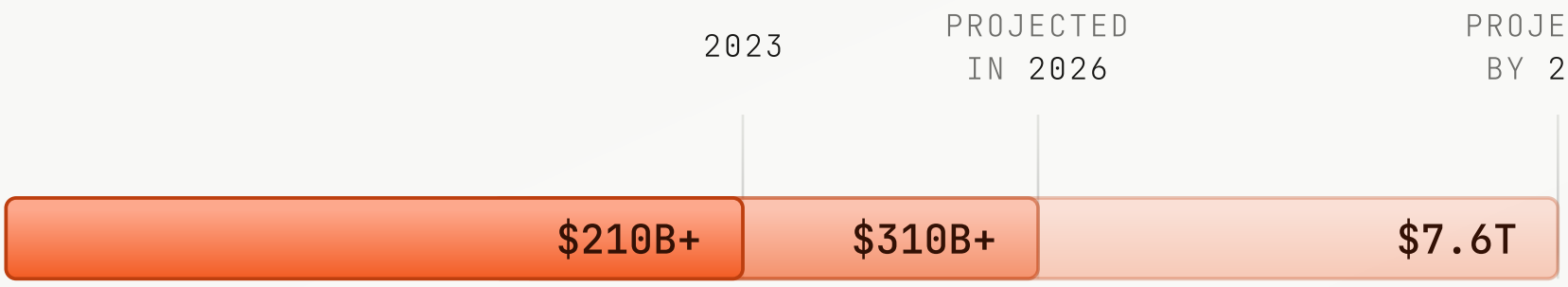
## Scale now signals maturity

This shift isn't limited to a few markets. Globally, neobanking adoption has accelerated rapidly. According to Simon-Kucher, the number of neobanking customers worldwide has reached approximately 1.1 billion, representing more than 30% growth in just 18 months.

Transaction volume tells an even larger story. By 2032, neobanks are projected to process more than $3.4 trillion in global transactions, with the market growing at an average annual rate of 48.9%. This level of throughput places digital-first banks firmly within the core infrastructure of global finance, not at its margins.

That reach is also becoming more concentrated. Today, more than 20 neobanks globally serve over 10 million customers each, placing several digital-first institutions among the largest banks in their home markets. Former challengers now operate at a scale demanding institutional-grade resilience and risk management.

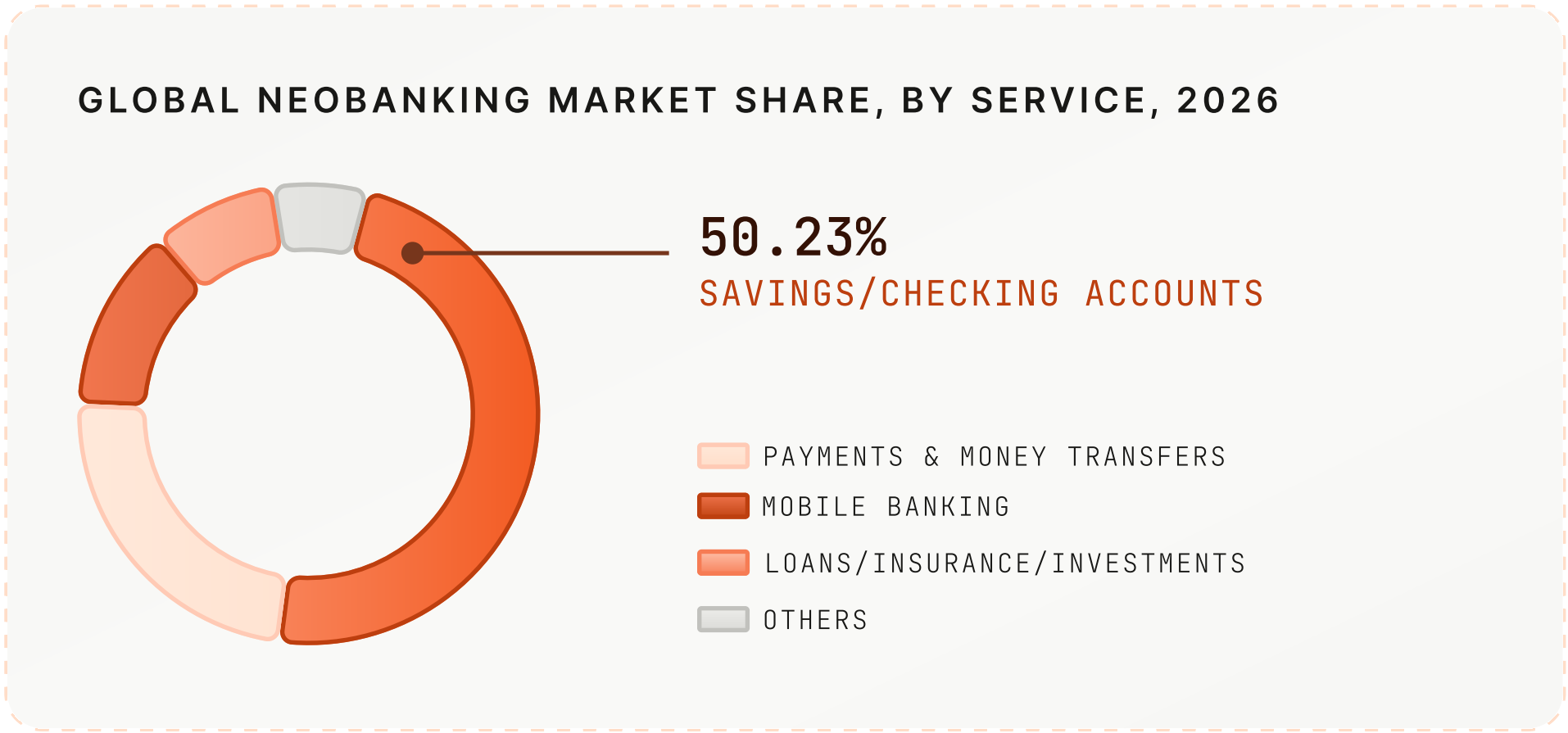
### THE NEOBANKING MARKET IS SCALING AT INSTITUTIONAL SPEED




SOURCE: FORTUNE BUSINESS INSIGHT, BANKING FINANCIAL SERVICES & INSURANCE MARKET RESEARCH REPORT, NEOBANKING MARKET, 2026

## Expansion raises the bar for trust

As neobanks move from fast growth to long-term relevance, many are expanding beyond their original propositions. Broader product suites, embedded financial services, and strategic partnerships are becoming common as platforms work to deepen engagement and increase lifetime value.




Savings and checking accounts remain the largest service category, accounting for 50.23% of the market share in 2026. However, payments, lending, investments, mobile banking, and emerging BNPL offerings now represent a significant and growing share of activity.

Multiple financial services now coexist within a single digital experience. Identity, fraud risk, underwriting, payments, and compliance oversight are no longer isolated functions. They intersect across products and channels.

As neobanks become central financial providers, they're increasingly held to institutional standards for resilience and risk management.

## Maturity changes the shape of risk

Controls that worked when accounts were small, lightly used, or treated as secondary begin to show their limits when activity becomes continuous and central to customers' financial lives.

As neobanks cross this threshold, fraud and abuse are no longer isolated operational issues. They become indicators of how well an institution can support growth without eroding trust, setting the stage for where pressure builds first and why traditional approaches increasingly struggle.

## Scale and speed have reshaped the fraud surface

As neobanks operate at higher velocity and volume, fraud evolves alongside them.

Fully digital onboarding, real-time payments, and always-on access are core to the neobanking experience. They reduce friction for legitimate users and make it easier to move money quickly; however, they also compress detection windows and give attackers more opportunities to test, refine, and repeat abuse.

### Speed tightens the window for response

Speed is the key accelerant. Instant payments adoption is increasing rapidly, and transaction sizes are growing with it. In Q2 2025, the RTP® network, operated by The Clearing House, processed $481 billion in payments in the U.S., a 195% increase in value from the previous quarter.

As larger sums move through real-time rails, the margin for delayed review narrows further. Once funds are in motion, response options are limited.

### Fraud now spans the full customer journey

As payments and access move faster, fraud no longer stays contained within a single step. What once surfaced at login or during a transaction now often begins earlier, before an account is fully established, and unfolds across messaging, onboarding, and payments.

By the time suspicious activity becomes visible, money may already be moving quickly.

### Interconnected products increase exposure

Growth also brings complexity. As user bases expand and product offerings broaden, so does the number of touchpoints where trust must hold. Financial activity that once lived in separate systems is now tightly integrated within a single platform, often including embedded lending and BNPL offerings.

These lending layers introduce new identity, underwriting, and repayment risks. When fraud touches credit decisions or installment payments, exposure extends beyond a single transaction and into regulatory and compliance obligations.

Each new capability adds value for customers, but also introduces new pathways for abuse when risk signals remain fragmented across systems.

This is where many traditional approaches start to break down. Controls designed around isolated events or checkpoints struggle in fast, interconnected environments. Even when teams recognize familiar patterns, the lack of continuity across sessions, accounts, or devices makes it difficult to connect signals early enough to prevent losses.

The result is a broader, more dynamic fraud surface. Understanding how speed, complexity, and fragmentation interact matters because they determine where pressure builds first and why many fraud prevention teams are forced into reaction instead of prevention.

## Why onboarding concentrates risk earlier than teams expect

For many neobanks, onboarding is treated as a compliance checkpoint: verify identity, approve the account, and move users into the product as quickly as possible. In practice, however, that framing breaks down. Onboarding decisions do more than approve or reject an applicant; they also determine how much trust an account receives, how quickly limits increase, and how freely money can move once the account is live.

### Onboarding is where trust is first assigned

Because onboarding sets the initial trust boundary, it becomes one of the most concentrated points of fraud risk. Passing early checks unlocks broader account access with minimal friction, giving attackers a strong incentive to succeed at this stage rather than later in the journey.

The risk is amplified in BNPL environments. Unlike traditional bank onboarding, BNPL sign-up happens at checkout, in the middle of a purchase. Customers are presented with a financing option and expect an almost instant decision.

At that moment, the platform is making a real trust decision. Based on a small set of submitted details, typically personal information and a soft credit pull, it decides whether to extend credit immediately. To preserve conversion, those checks are streamlined. The goal is to confirm that the information appears legitimate, not to deeply investigate the identity behind it.

And that's where the exposure sits. Data matching can confirm that details look consistent. It can't confirm that the identity itself wasn't synthetically constructed.

Synthetic identities are built to exploit exactly this moment. By combining real and fabricated information, such as a valid Social Security number coupled with a slightly different name and fake address, fraudsters create profiles that pass validation while hiding intent. In installment models, those accounts may look legitimate at approval but later default or support coordinated abuse.

The Deloitte Center for Financial Services estimates that synthetic identity fraud will generate at least $23 billion in losses by 2030, highlighting how costly early-stage abuse can become.

Synthetic identity fraud projected to exceed

**$23B in losses by 2030**

SOURCE: THE DELOITTE CENTER FOR FINANCIAL SERVICES, 2025



## Point-in-time checks leave a structural gap

The challenge is that onboarding checks are typically isolated event checks by design. They answer a narrow question, “Does this applicant meet requirements right now?” without accounting for how behavior may change minutes or hours later.

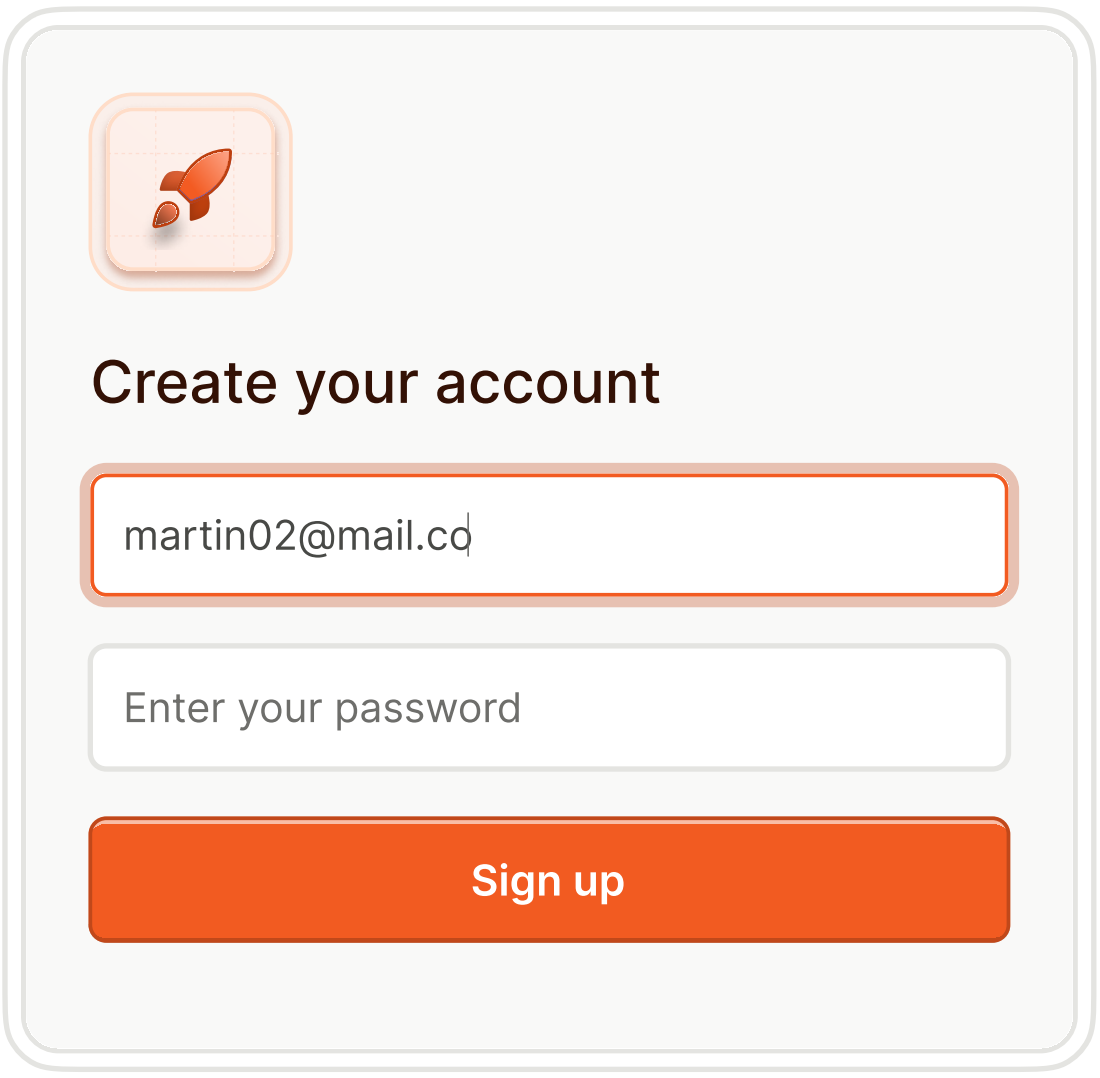
In fast-moving environments, that gap matters. An account that appears low-risk at signup can become high-risk shortly after, particularly when instant payments or installment credit are available. When verification is treated as a pass-or-fail step, risk visibility resets at the very moment trust is extended.

## Growth pressure complicates early risk decisions

Onboarding remains one of the most visible moments in the customer experience. Digital banks compete on ease of use, and every additional verification step risks slowing conversion.

Without strong signals that persist beyond signup, teams are forced to make trade-offs between growth and control. Those early trust decisions shape how quickly risk can escalate and how difficult it is to intervene later.

That’s why onboarding has become a focal point for modern fraud: not because it’s the only place abuse occurs, but because it sets the conditions for everything that follows.

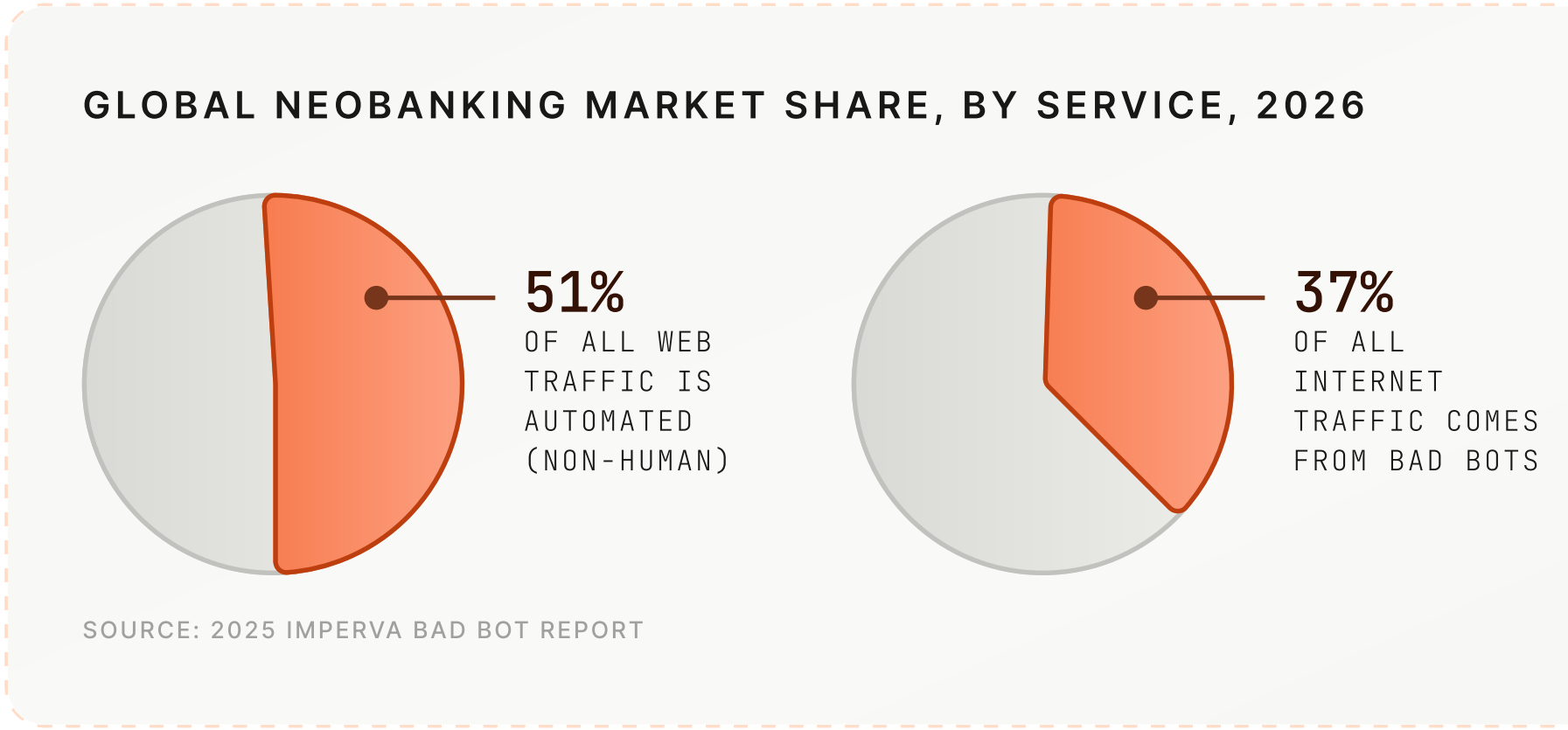


## How AI and automation industrialize early-stage abuse

As onboarding becomes faster and more automated, attackers no longer rely on isolated tactics. They operate industrially, using AI and automation to probe, reuse, and scale whatever works.

### Automation turns onboarding into a volume game

Automated traffic now accounts for more than half of all global online activity, making large-scale, repeatable abuse easier to hide inside legitimate demand.




In financial services, these bots increasingly mimic legitimate users while exploiting business logic rather than technical vulnerabilities. Credential testing, document submission, and recovery flow probing can be executed at scale and masked within normal traffic patterns.

Onboarding, designed for speed and conversion, becomes an efficient testing ground.

### AI makes successful patterns repeatable

AI accelerates this exploitation. Synthetic identities can now be assembled and refined quickly, combining real data with fabricated details that pass basic checks. Documents can be altered, reused, or regenerated at scale. Emulator farms allow attackers to simulate thousands of “unique” users, making automated account creation harder to distinguish from genuine demand.

Once a tactic succeeds, it doesn’t stay isolated. It becomes a reusable template.

## Incentives accelerate coordinated abuse

Incentives and promotions amplify the problem. Signup bonuses, referral rewards, and early-access features create immediate value for newly opened accounts — value that fraudsters are quick to extract. Instead of a single account behaving badly, teams may face waves of coordinated signups, each designed to look benign in isolation but harmful in aggregate.

By the time unusual payment behavior appears, the underlying weaknesses have already been exploited. Trust has been extended. Limits have increased. Accounts have aged just enough to blend in.



## Scams now drive fraud outcomes, not just transactions

Fraud in neobanking environments is no longer defined by system failures. Increasingly, it's driven by scams — coordinated schemes that manipulate users into moving their own money.

The scale of this shift is measurable. The Veriff Identity Fraud Report 2023 identified a 17.9% increase in fraudulent activity across financial services over the past year, highlighting the industrial scale of modern fraud. Increasingly, organized crime groups are using phishing and coordinated infrastructure to compromise accounts at volume, not as isolated incidents.



**17.9% increase**

in fraudulent activity across financial services

SOURCE: VERIFF IDENTITY FRAUD REPORT 2023

### Scams turn legitimate journeys into fraudulent outcomes

Impersonation, investment, romance, and job scams continue to grow because they don't rely on breaking controls. Instead, they exploit trust. Attackers pose as employers, support agents, government officials, or romantic partners, guiding victims step by step toward an action that appears legitimate in the moment. By the time a payment is made, the user believes they are doing the right thing.

### Messaging platforms are where scams begin

Messaging platforms have become the primary attack vector for these scams. Conversations unfold over SMS, email, and popular messaging apps, often entirely outside banks' visibility. The fraud itself doesn't begin at the payment screen. It begins days or weeks earlier, as attackers build credibility, apply pressure, and create a sense of urgency or authority.

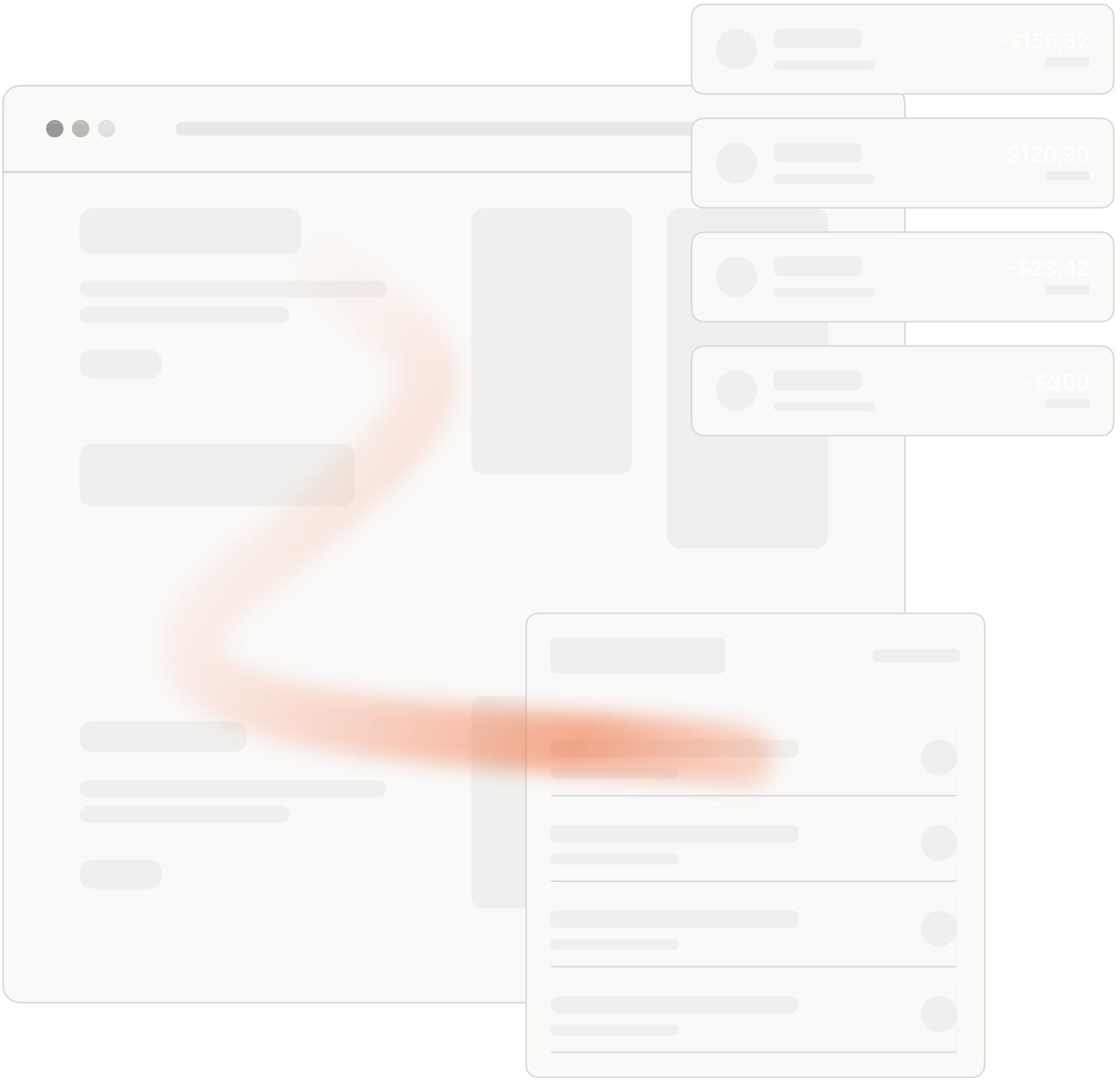
### Low-friction experiences increase scam success

What makes scams especially effective in neobanking environments is how well they align with low-friction design. Fast onboarding, instant access to payments, and real-time transfers are features customers value. In scam scenarios, those same features reduce the opportunity to pause, question intent, or intervene before funds are sent.

## Scams coordinate onboarding, access, and payments

Scams also coordinate multiple stages of the account lifecycle. Accounts created or aged through earlier abuse can be used to receive funds. Compromised or newly opened accounts may act as intermediaries. Payments move quickly across rails designed for speed, not reversal. From a systems perspective, each action may look authorized.

This is why scams now dominate fraud outcomes. They blur the line between fraud and authorized activity, shifting responsibility and complicating response. Traditional transaction-based controls struggle because the payment itself looks legitimate.



## Authorized push payment (APP) fraud puts trust under a microscope

Authorized push payment (APP) fraud, where scammers convince customers to authorize a transaction, sits at the uncomfortable intersection of scams, payments, and accountability. Because the transaction is authorized by the customer, it's often irreversible. As a result, APP fraud exposes gaps that are harder to remediate and harder to defend.

### APP fraud exploits legitimate user authorization

Unlike traditional payment fraud, APP scams don't rely on compromised credentials or unauthorized access. The user approves the payment with valid credentials, and systems behave exactly as designed because, from a transactional perspective, nothing looks wrong.

The end result: Responsibility becomes harder to assign when authorization is legitimate, but intent is manipulated. Fraud controls built to detect anomalies at the point of payment often struggle in such cases because the payment itself doesn't deviate from expected behavior.

### Real-time payments leave little room for reaction

The rise of real-time and instant payments has amplified this challenge. Once funds are sent, recovery windows shrink dramatically or disappear altogether. There is little opportunity to pause, investigate, or reverse a transaction after it's been authorized.

In the United States, losses from APP fraud are estimated to rise from $8.3 billion in 2024 to $14.9 billion by 2028 under baseline assumptions. In more aggressive scenarios, where AI-driven scams outpace institutional and societal defenses, losses could reach as much as $18.2 billion over the same period.



### Consumer harm is immediate and highly visible

APP fraud also carries a different kind of impact. Losses are personal, often involving investment funds, business payments, or life savings. Notably, investment scams are expected to account for the largest share of projected APP fraud growth, followed by bank and business impersonation and romance scams, categories that rely heavily on trust-building rather than technical compromise.

For customers, the distinction between “authorized” and “unauthorized” is irrelevant. They experience the loss directly and expect their financial institution to help, regardless of how the fraud occurred.

### Regulators are shifting focus from detection to prevention

As APP fraud volumes rise, regulatory attention is following. Expectations are expanding beyond whether fraud was detected to how effectively it was prevented. Regulators are increasingly examining:

- Whether institutions apply preventative controls earlier in the customer journey
- The quality and consistency of detection across channels and payment types
- How reimbursement decisions are handled when customers are manipulated rather than hacked

This shift reflects a broader reality: when fraud reaches payments, it’s no longer just a fraud problem. It becomes a trust and compliance problem.

This is why APP fraud has become such a defining challenge for neobanks. It forces teams to reconcile speed with safety, authorization with intent, and growth with accountability, often under intense public and regulatory scrutiny.

## Account takeover and mule networks move faster at scale

As neobanks and BNPL providers grow, fraud compounds. Accounts compromised through earlier abuse are quickly reused, repurposed, and cycled through broader networks designed to move money before controls can respond.

### Account takeover has adapted to low-friction environments

Account takeover hasn't disappeared in digital-first banking. It has adapted to it. Traditional account takeover once relied heavily on stolen credentials and password reuse. Today, attackers increasingly bypass basic safeguards altogether. SMS one-time passwords, weak biometric checks, and static recovery flows are routinely tested and exploited in environments optimized for speed.

In BNPL environments, the incentives are even sharper. Fraudsters increasingly target established, trusted installment accounts, especially those with strong payment histories and higher spending limits. These accounts have already shown on-time payments and low-risk, making them more likely to pass automated approval checks.

Once access is gained, attackers move quickly. High-value purchases are made with new merchant accounts and shipped to new addresses that don't match prior behavior. Because the account carries a history of legitimate activity, those transactions may not immediately trigger suspicion.

The fraud often surfaces later, when the legitimate customer notices unfamiliar charges and files a dispute or chargeback. By that point, goods have shipped, merchants absorb losses, and recovery options are limited.

In digital-first banking and BNPL, speed is a customer expectation. But real-time payments, instant approvals, and streamlined recovery flows reduce the window for intervention. By the time unusual activity surfaces, funds may already be dispersed and goods delivered.

### Mule networks prioritize speed and turnover

Money mule activity has become more efficient as platforms scale. Mule accounts tend to be short-lived, high-velocity, and disposable by design. Once an account has served its purpose (receiving funds, moving money onward, or obscuring the source), it's abandoned and replaced.

This high turnover makes mule networks difficult to detect using traditional indicators. Individual accounts may appear unremarkable in isolation. Patterns only emerge when behavior is observed across accounts, sessions, and devices, something point-in-time checks struggle to see.

The speed of these networks reflects broader changes in payment infrastructure. As instant payments adoption rises and transaction limits increase, compromised accounts can be drained and repurposed within minutes, reducing recovery windows and increasing loss velocity.

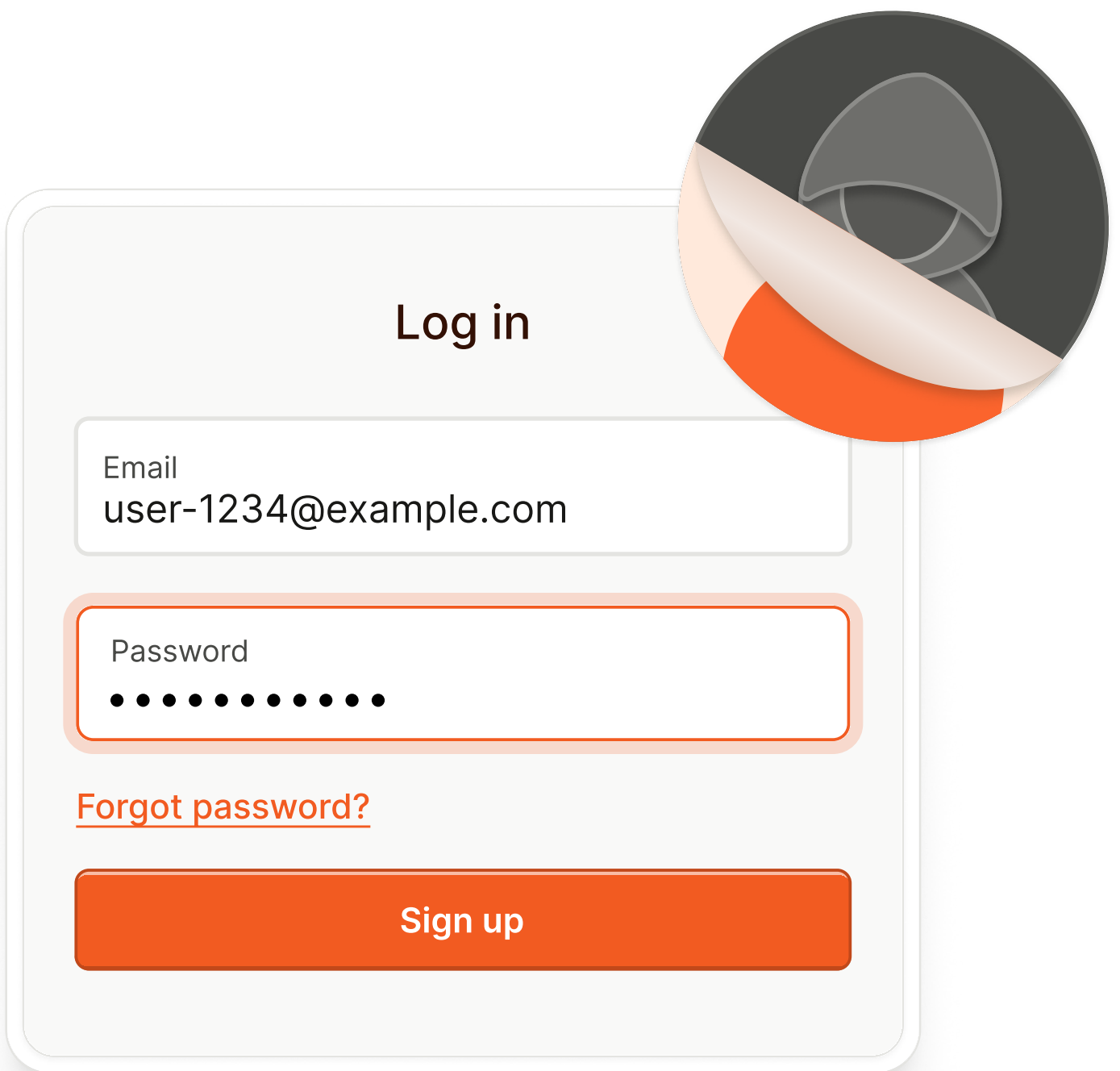
## Compounding abuse exposes the limits of point-in-time controls

What links modern account takeover and mule activity is repetition. The same techniques, infrastructure, and behavioral patterns are reused across accounts at speed. Yet many controls remain focused on single events: a login, a transaction, a password reset.

In scaled environments, that approach breaks down. Point-in-time checks can confirm access, but they struggle to identify coordinated behavior unfolding over time. By the time repeat abuse becomes visible, money has often already moved through multiple accounts and platforms.

This compounding effect is what makes later-stage fraud so difficult to contain. Each missed signal increases downstream exposure, not just for a single customer, but across the broader network of accounts connected by shared infrastructure and behavior.

At scale, the challenge is connecting repeat behavior early enough to intervene before funds move.



## When fraud becomes a compliance constraint

Many neobanks operate through banking-as-a-service partnerships or licensed institutions. When fraud failures occur, accountability may span multiple entities, increasing regulatory complexity and reputational exposure.

As abuse compounds across accounts, channels, and products, it stops looking like isolated fraud and instead becomes a compliance issue, often long after the original failure occurred.

### Fraud failures surface as anti-money laundering (AML) issues

Many of the signals compliance teams investigate are downstream effects of fraud that began earlier in the customer lifecycle. Suspicious transaction patterns, unusual account activity, and rapid fund movements often trace back to onboarding decisions, compromised accounts, or scam-driven payments that were never fully understood in context.

From an anti-money laundering (AML) perspective, this creates a difficult dynamic. Activity may technically comply with transactional rules while still representing elevated risk. Accounts may pass initial screening yet later behave in ways that trigger monitoring thresholds, forcing compliance teams to react to symptoms rather than causes.

### BNPL expands regulatory and fraud exposure

BNPL is becoming a structural layer of digital finance. Thus, BNPL exposes the same trust gap as neobank onboarding, but with underwriting and repayment layered in.

The global BNPL market was valued at $44.9 billion in 2025 and is projected to reach $286 billion by 2034, growing at a 23% compound annual rate. As installment-based lending expands inside neobank ecosystems, so does its exposure to fraud and compliance risk.

Fraud rates in BNPL transactions now range between 1.5% and 6% of transaction volume, up to six times higher than traditional credit card fraud rates. Retailers alone are estimated to lose $3 to $5 billion annually to BNPL-related fraud. When investigation costs, chargebacks, and operational strain are included, the total economic impact exceeds $10 billion per year.

The risk profile is evolving.

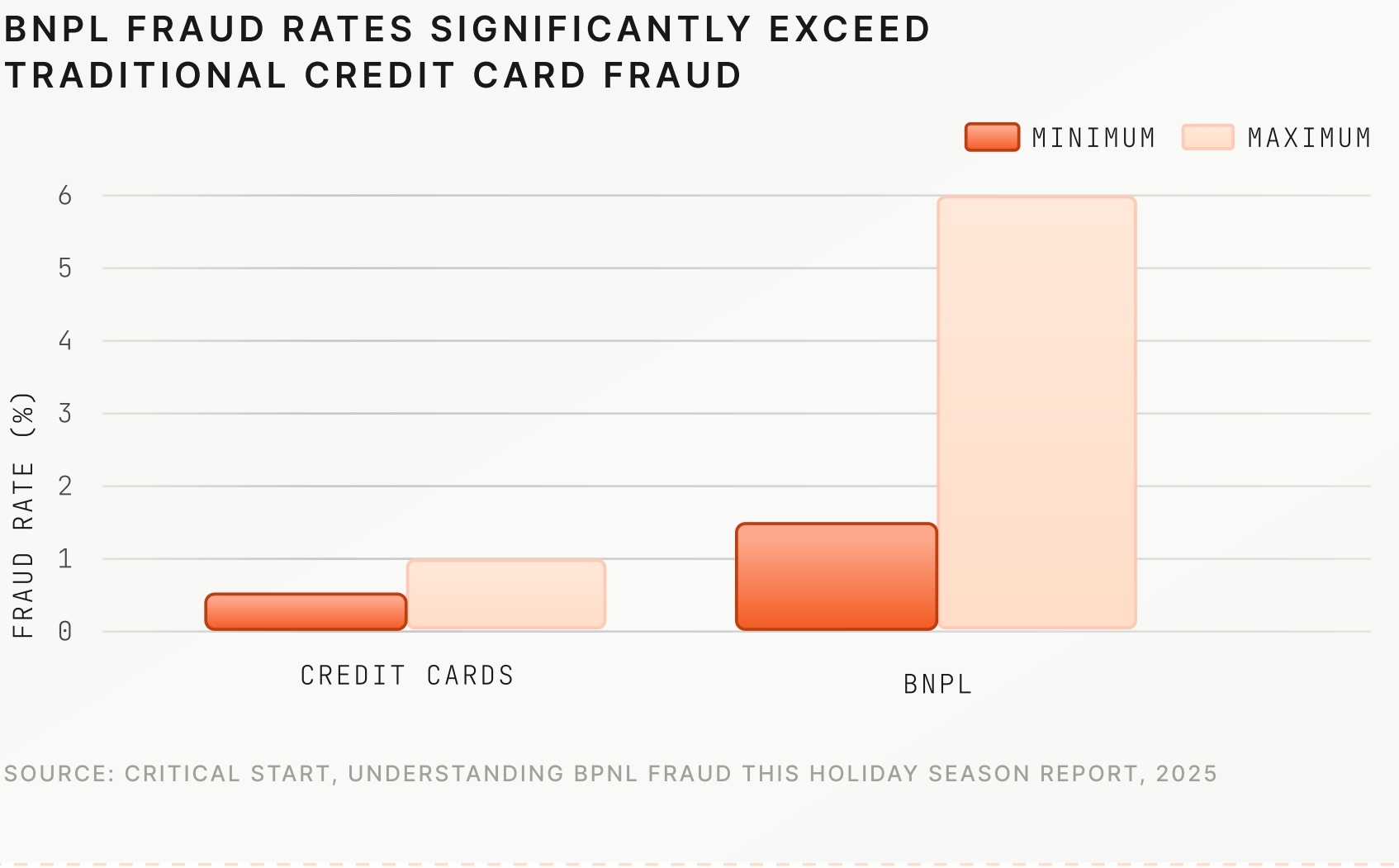
New account abuse represents nearly 28.8% of recent fraud activity, reflecting the same early-stage vulnerabilities seen in digital banking onboarding. Fraud methods now include mature synthetic identities, AI-generated documents, and account takeovers targeting pre-approved installment lines.

At the same time, delinquency trends introduce additional exposure. Between 34% and 41% of BNPL users made a late payment in the past year, with Gen Z delinquency rates reaching 51%. While not all late payments represent fraud, weak identity and risk signals blur the line between credit risk, first-party misuse, and organized abuse.

When identity signals are fragmented, the impact extends beyond transaction loss. It affects:

- Underwriting accuracy
- AML monitoring
- Regulatory reporting
- Merchant liability exposure

In digital finance, lending risk and fraud risk are no longer separate conversations. And when lending, fraud, and compliance signals remain fragmented, monitoring pressure intensifies downstream.




SOURCE: CRITICAL START, UNDERSTANDING BPNL FRAUD THIS HOLIDAY SEASON REPORT, 2025

## Poor signal quality increases alert noise

As fraud patterns grow more coordinated, monitoring systems generate more alerts, but not necessarily better ones. When signals lack continuity across sessions, accounts, or devices, alerting becomes noisy and fragmented. Compliance teams are left sorting through large volumes of low-confidence flags, trying to distinguish real risk from false positives.

This noise has real consequences. Investigations take longer. Backlogs grow. Analysts spend more time validating benign behavior, while genuinely risky activity may blend into the background.

Rules-based monitoring can generate

**false positive rates above 95%**

SOURCE: FINTECH GLOBAL, APRIL 2025

**HIGH ALERT VOLUME** DOES NOT EQUAL EFFECTIVE DETECTION.

## Operational strain affects customers and retention

The impact isn't limited to internal teams. Increased alert volume often leads to more reviews, holds, or follow-up requests that customers experience as friction or confusion. Legitimate users may face delays, repeated verification, or account restrictions without clear explanation.

Over time, this erodes trust. Customers who chose neobanks for speed and simplicity are confronted with processes that feel inconsistent or opaque. What begins as a fraud-control issue becomes a customer experience and retention risk.

## Regulatory scrutiny focuses on monitoring quality, not alert volume

Regulators are paying closer attention to how institutions monitor and manage risk, not just how many alerts they generate. The expectation is shifting toward effective, consistent monitoring that reflects an understanding of behavior over time, rather than reliance on volume-driven thresholds.

Enforcement actions are reinforcing this shift. In the UK, the Financial Conduct Authority fined a leading neobank £28.9 million for failures in AML and sanctions screening, underscoring that digital-first institutions are now held to the same standards as established banks.

In this environment, excessive alerts aren't a sign of strength. They can indicate weak signal quality, fragmented visibility, or controls that struggle to adapt to modern fraud patterns.

## Compliance teams feel the downstream impact of upstream fraud

As neobanks scale, the line between fraud prevention and compliance continues to blur. Preventing abuse earlier in the lifecycle reduces losses and keeps monitoring, investigations, and regulatory oversight manageable as platforms grow.

## The growth vs. friction dilemma neobanks can’t avoid

For many neobanks, growth and low friction have been inseparable. Fast onboarding, minimal verification, and instant access to products helped fuel adoption and differentiate digital-first platforms from traditional banks. Those same design choices now sit at the center of a difficult tradeoff.

### Growth pressure favors low friction

Neobanks often operate on thinner margins than incumbents, with growth targets tied closely to acquisition, activation, and engagement. Every added step in onboarding or account access risks reducing conversion, slowing time to value, or increasing abandonment. As a result, friction is closely scrutinized and often resisted even when risk signals suggest caution.

This pressure isn’t theoretical. Onboarding and early account activity are among the most visible moments in the customer journey, shaping first impressions and long-term retention. Teams are understandably hesitant to introduce controls that could undermine those experiences.

### Fraud losses and false positives both hurt unit economics

Fraud pressure now affects more than security teams. It directly impacts growth, margin, and long-term customer value.

According to the U.S. Fraud Industry Pulse Survey 2025:

- 72% of businesses report year-over-year increases in online fraud
- 75.5% report direct revenue loss
- 32% report a 3–5% reduction in revenue tied to fraud

Missed fraud increases direct financial losses, reimbursement exposure, chargebacks, and operational overhead. At scale, even small percentage shifts materially affect margins.

Excessive friction creates a different but equally costly drag. When legitimate users are challenged, delayed, or declined unnecessarily, conversion rates fall, support costs rise, and lifetime value erodes.

In BNPL and installment lending models, this tension becomes sharper. Approval speed directly impacts merchant conversion and revenue. Every additional verification layer can reduce checkout completion rates. At the same time, weak upfront identity signals increase exposure to synthetic identities, first-party misuse, and repayment abuse. When fraud prevention and underwriting rely on incomplete context, institutions are forced into tradeoffs that don’t scale.

The result is a compounding effect on unit economics. Fraud increases losses. Friction reduces growth. And without better signals, both costs rise simultaneously.

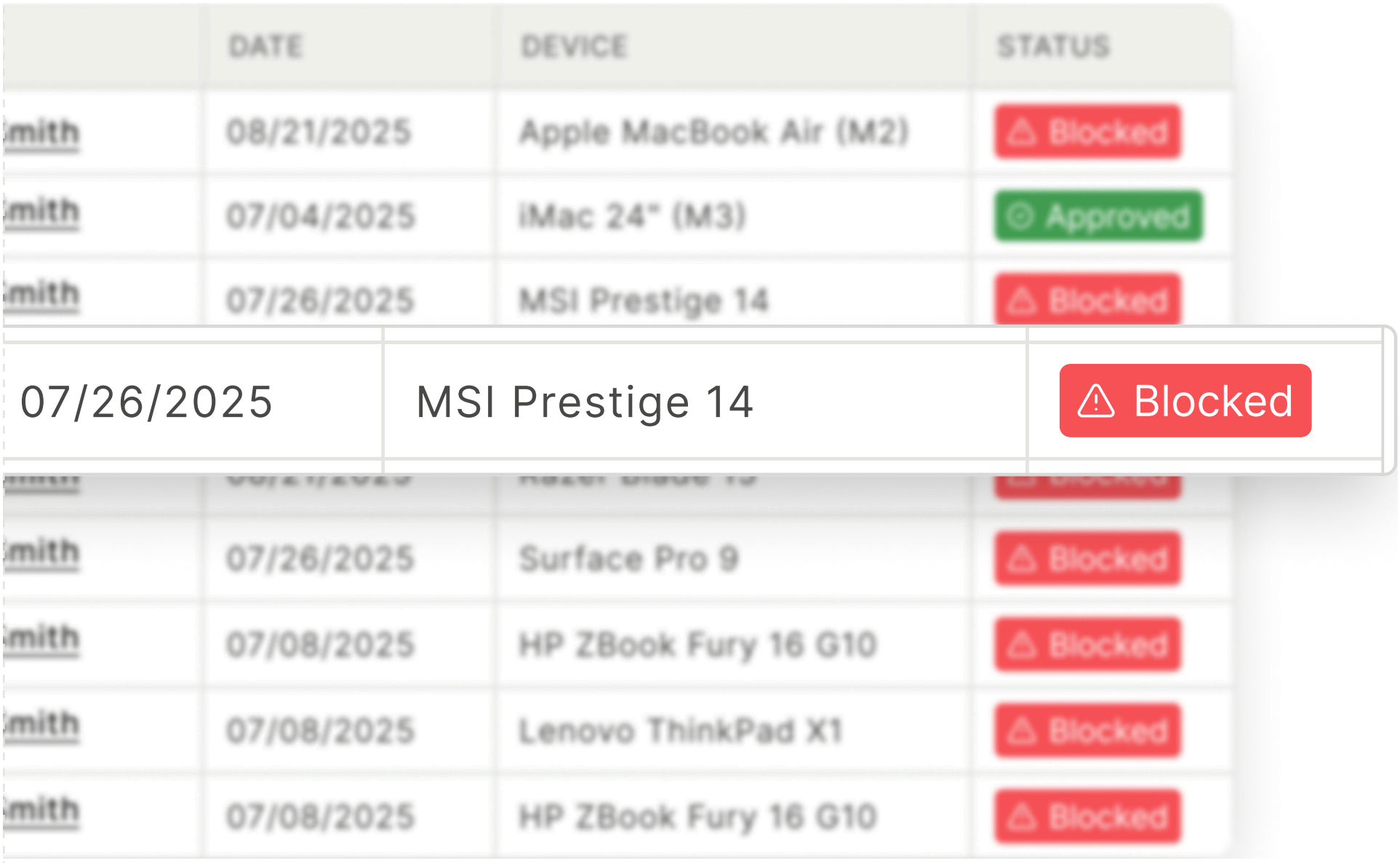
### Blocking more users doesn’t scale

Faced with rising fraud pressure, some teams respond by tightening controls broadly, lowering thresholds, adding manual reviews, or slowing access across the board.

But as platforms grow, blanket friction becomes increasingly expensive. Legitimate customers feel the impact first, while determined attackers adapt, reroute, or wait out restrictions. Over time, the organization pays more to achieve diminishing returns.

The underlying problem isn’t the presence of fraud controls. It’s that they’re often applied uniformly, without enough context to distinguish between high-risk and low-risk behavior early enough to matter.

This dilemma is unavoidable for neobanks operating at scale. Success means finding ways to manage risk that protect both.



## What conversion-safe fraud prevention actually requires

As neobanks scale, the limits of traditional fraud prevention become harder to ignore. Adding more rules, more thresholds, or more manual reviews may feel like progress, but it rarely delivers better outcomes. In fast-moving, digital-first environments, complexity often creates noise without meaningfully reducing risk.

### More rules don’t equal better outcomes

Rule-based systems were built for predictability. They work best when behavior is stable, transactions are infrequent, and risk changes slowly. None of those conditions hold in modern neobanking environments.

As fraud patterns evolve, rule stacks grow more complex, and exceptions multiply. Thresholds are tuned and retuned. Yet attackers adapt faster than static logic can keep up. The result is a familiar pattern: rising false positives alongside persistent fraud losses.

### Better signals outperform complex rule stacks

What separates effective fraud prevention from reactive control is signal quality. For example, signals such as repeated device use across supposedly unrelated accounts, or patterns that persist across sessions, are often early indicators of organized fraud.

When signals are weak or fragmented, teams compensate with more rules. When signals are strong and consistent, fewer interventions are needed to achieve better outcomes, protecting conversion without sacrificing control.

### Continuity matters more than checkpoints

Many fraud programs still rely on checkpoints: onboarding, login, and payment. Each step is evaluated in isolation, often by different systems. This approach creates gaps that attackers exploit by moving between stages faster than controls can adapt.

Conversion-safe prevention depends on continuity. Risk signals need to persist across sessions and link behavior across accounts, allowing models to learn from patterns rather than isolated events. Without that continuity, credentials can confirm access, but they can’t confirm intent.

### Early intent signals change the tradeoff

The earlier risk can be assessed with confidence, the fewer tradeoffs teams have to make later. Signals that surface repeat behavior, shared infrastructure, or coordinated patterns allow institutions to intervene selectively, before limits rise, before funds move, and before customers are impacted.

This is the shift required to escape the growth-versus-friction dilemma — not by slowing everyone down, but by identifying when and where speed itself is the risk.

## How device intelligence supports trust at scale

At scale, trust can’t be rebuilt at every step. It has to carry forward. This is where device intelligence becomes a critical layer in modern fraud prevention for neobanks, providing continuity across the customer lifecycle without adding friction for legitimate users.

### Persistent insight across the full customer journey

Fraud rarely confines itself to a single moment. The same devices and infrastructure often appear across onboarding, account access, scams, and payments. Device intelligence makes those connections visible by providing persistent insight that travels with the user journey, rather than resetting at each checkpoint.

Instead of evaluating onboarding, login, and payments as isolated events, teams can see how activity connects over time, and whether it reflects genuine new behavior or repeat patterns that signal organized abuse.

### Earlier detection of repeat and coordinated abuse

Repeat abuse is one of the strongest indicators of fraud at scale. Device intelligence helps surface this early by identifying when the same devices or environments reappear across multiple accounts, sessions, or attempts, often before limits increase or funds move.

This visibility allows teams to intervene selectively. High-risk activity can be slowed, challenged, or reviewed, while legitimate users continue uninterrupted. The result is earlier control without broad friction.

### Fewer false positives through adaptive risk

When risk decisions rely on static rules or single signals, false positives rise. Device intelligence improves precision by adding behavioral and environmental context to each interaction.

As patterns change, risk decisions can adapt with them. Legitimate users who move quickly aren’t automatically penalized, while coordinated abuse becomes easier to isolate. Over time, this reduces unnecessary reviews and customer-facing friction, protecting both experience and efficiency.

## Stronger inputs for existing machine learning (ML) systems

Device intelligence strengthens machine learning. By feeding models with consistent, high-quality signals across sessions and accounts, teams improve the accuracy and durability of their existing detection systems.

This is particularly valuable in BNPL and embedded lending models, where underwriting decisions must balance approval speed with fraud and repayment risk. Persistent device insight helps distinguish repeat misuse from legitimate new customers, strengthening both fraud prevention and credit decisioning without adding friction.

Models trained on fragmented data struggle to learn. With persistent signals, they adapt faster, improve accuracy, and make fewer costly mistakes as behavior changes.

## Supporting global scale and AML monitoring

As neobanks expand across regions and payment rails, consistency becomes harder to maintain. Device intelligence provides a stable signal layer that supports fraud prevention and AML compliance across regions, helping teams recognize repeat behavior even as users, networks, and regulations vary.

This continuity is especially valuable for compliance teams, where understanding behavior over time is critical to effective monitoring without overwhelming operations.

At its core, device intelligence helps neobanks manage risk without slowing growth. It strengthens the tools teams already use, adds context where it's missing, and supports trust as platforms scale.

Fingerprint is built to support this approach, strengthening existing fraud and compliance systems rather than replacing them, and helping digital banks protect trust without sacrificing conversion.

KEY TAKEAWAYS

# Trust is now infrastructure

Neobanking fraud in 2026 is no longer episodic or isolated. As digital-first banks scale, trust failures compound. What begins as a missed signal during onboarding can cascade into account takeover scams, payment losses, and regulatory scrutiny, often unfolding faster than teams can respond.

This shift has changed what effective fraud prevention looks like. Isolated event checks and siloed controls struggle in environments defined by speed, interconnected journeys, and continuous use. Slowing everyone down isn't a viable solution, and neither is reacting after money has already moved.

The banks that succeed at scale treat trust as infrastructure. They invest in signals that persist across sessions and products, surface repeat behavior early, and adapt as risk evolves, without adding unnecessary friction for legitimate users.

In that model, fraud prevention isn't a brake on growth. It's what makes sustainable growth possible.

As neobanks continue to mature, the challenge isn't choosing between speed and safety. It's building systems that support both, so trust keeps pace with innovation, and customers can rely on their bank not just to move money quickly, but to protect it consistently.

### Protect trust without slowing growth

Learn how Fingerprint's device intelligence helps digital banks reduce fraud, lower false positives, and scale safely, without adding friction for legitimate users.

Start a free trial | Contact sales


### About Fingerprint

**Fingerprint detects the intent of human and agentic visitors.**
Our device intelligence platform identifies over 1 billion unique devices every month and processes hundreds of signals to help fraud teams distinguish trusted visitors from bad actors at speed and scale. Over 6,000 companies, including innovators like Dropbox, Booking.com, and checkout.com, use Fingerprint every day to recognize high-risk activity in real time, prevent fraud attacks, and deliver frictionless user experiences. **Learn more at** fingerprint.com.