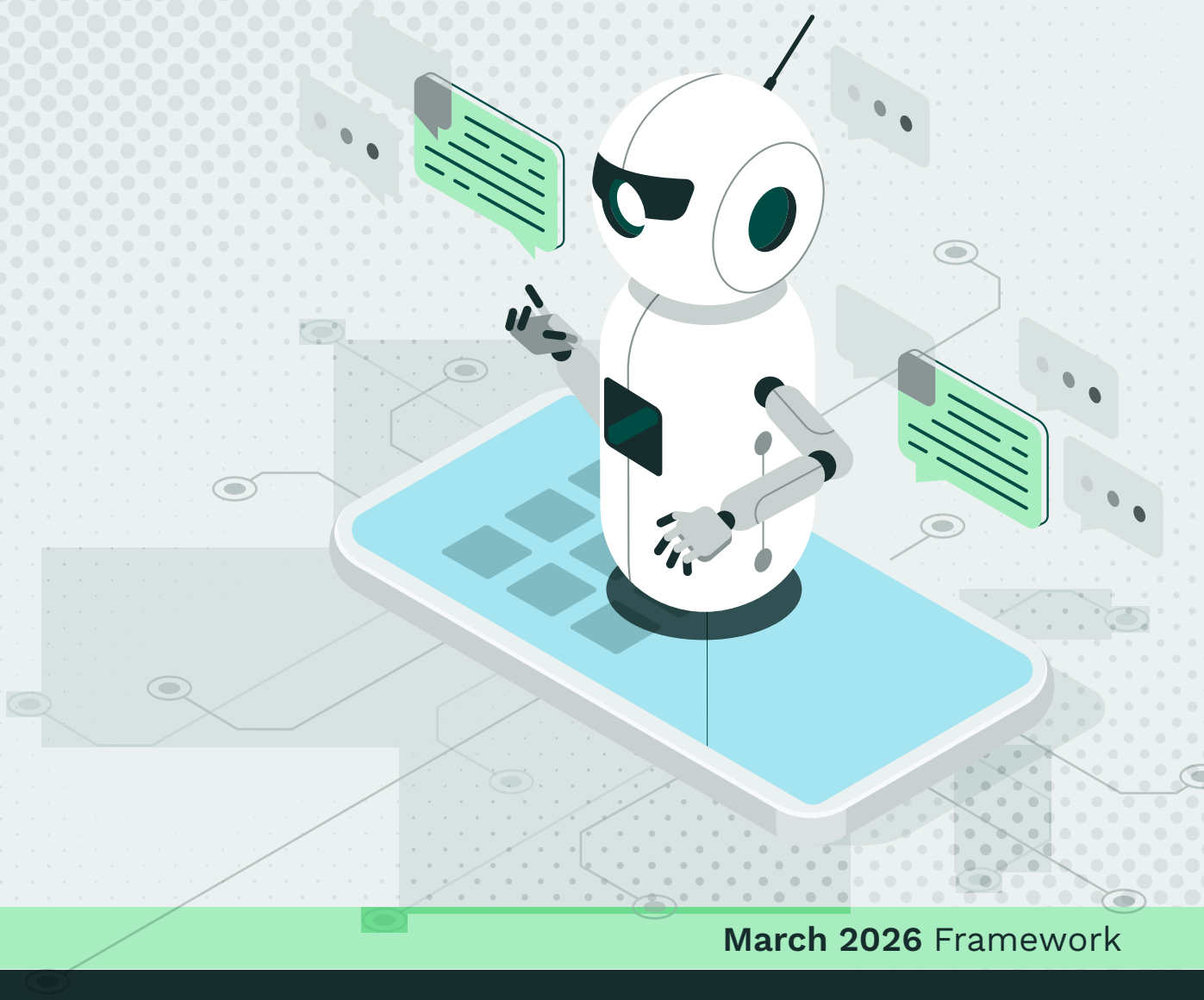


March 2026 Framework

How Enterprises Can Build a 'Know Your Agent' Defense

Digital Identity Verification in the Age of Bots

PYMNTS INTELLIGENCE

How Enterprises Can

Build a ‘Know Your Agent’ Defense

READ MORE

January 2026

When ‘Good Enough’ Isn’t Enough:
Digital Identity Verification in the Age of Bots and Agents

PYMNTS INTELLIGENCE | Trulioo

How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots was produced in collaboration with Trulioo, and PYMNTS Intelligence is grateful for the company’s support and insight. PYMNTS Intelligence retains full editorial control over the following findings, methodology and data analysis.

Table of Contents

Executive **Summary**

For decades, an enterprise’s digital security strategy was built on a simple assumption: that the internet is driven by people interacting with other people. Every firewall, login screen and fraud detection model was designed with the expectation that a human being was sitting on the other side of the connection.

In 2024, that era quietly ended. Automated traffic surpassed human activity for the first time, accounting for 51% of all web interactions, according to Imperva’s 2025 Bad Bot Report. What’s more, this new majority is increasingly hostile. Malicious bots now comprise 37% of the total volume, the sixth consecutive year of growth. As agentic commerce gains traction, distinguishing bad bots from legitimate automated agents shopping for groceries, booking travel, managing subscriptions, negotiating contracts and initiating payments on behalf of consumers and suppliers is now an existential challenge for global platforms and marketplaces.

Know Your Agent can’t exist without strong KYC and KYB. But when that underlying identity infrastructure is weak, no amount of agent detection will prevent sophisticated abuse. **In the age of bots and agentic commerce, “good enough” verification systems are a liability.**

What’s clear amid that challenge is that a core level of the three processes for identity verification—know your customer (KYC), know your business (KYB) and know your agent (KYA)—isn’t working well. KYA-related adversarial incidents and losses over 12 months through September 2025 hit 57% of enterprises with more than $1 billion in revenue, compared to 32% among smaller firms, PYMNTS Intelligence data shows. In a KYA environment, large-scale and cross-border complexity boost the odds of “good enough” identity verification controls both missing bad actors and misclassifying legitimate customers, heightening operational drag.

As scale increases, the manual effort and customer frustration required to resolve **“good enough” control failures become a significant drag on growth.**

Amid the automated onslaught, up to 99% of firms with less than $1 billion a year in revenue feel relatively secure in their ability to distinguish between a helpful AI assistant and a digital thief. But only 91% of $1 billion-plus enterprises have that same confidence. And when enterprises can’t routinely distinguish between a “bad” bot and a “good” agent (or an actual human), they end up blocking legitimate users. PYMNTS Intelligence finds that among companies with at least $1 billion in revenue, the rate of false positives spikes to 3.3% of all transactions. That’s significantly above the 2.7% rate for companies with revenues of $50 million to less than $250 million, and 3.0% for firms with $250 million but less than $1 billion. Collectively, the losses due to fraud and missed opportunities cost businesses nearly $100 billion a year.

“Good enough” comes in many forms. Companies relying on in-house verification tools face high user drop-off and bot-driven losses, while third-party tools reduce false positives but constrain growth. Hybrids combining both become targets for credential stuffing and account takeovers.

These are just some of the findings detailed in How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, a PYMNTS collaboration with Trulioo. This edition examines how the rise of agentic bots is outpacing legacy identity controls, disproportionately exposing large enterprises to industrialized fraud and misidentification of legitimate customers. It draws on insights from a survey of 350 leaders in compliance, risk management, fraud, underwriting, supplier acquisition and merchant monitoring at global companies that was conducted from Aug. 1, 2025, to Sept. 10, 2025.

This is what we learned.

Key Findings

01

The bot juggernaut

Bot traffic increased for 52% of organizations in the past year alone. False-positive rates at large enterprises hit 3.3%, highlighting how legacy "good enough" controls are failing under dual pressure from adversarial bots and legitimate agent-driven commerce.

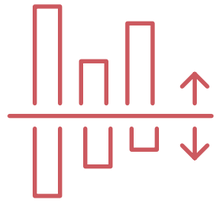
89.5%

of organizations now report that managing bot traffic is a challenge.

02

How KYA threats and losses scale

KYA adversarial incidents and fraud-related losses are disproportionately likely to affect companies with at least $1 billion in annual revenue.



57%

of enterprises with $1 billion or more in annual revenue experienced KYA-related incidents or losses over 12 months through September 2025. For smaller firms, the share was 32%.

03

AI industrializes $100 billion a year in lost revenue

"Good enough" KYB and KYA practices cost businesses nearly $100 billion annually in fraud and missed opportunities, with large firms mistakenly flagging 3.3% of legitimate users as malicious, compared to 2.7% at small firms.

$100B

is lost by companies each year due to fraud and inadvertent blocking of legitimate transactions.

04

Identity models drive KYA vulnerabilities and costs

53%

of companies that manage their identity operations internally face higher rates of KYA-related incidents/losses compared to companies deploying third-party provider models (24.1%) or hybrid models (28.8%).

05

The five-layer KYA model

Any weakness in the KYC or KYB layer, such as a synthetic or compromised identity, cascades directly into the KYA layer. This reinforces identity as a strategic variable in infrastructure built for an agentic economy rather than merely a control cost.

THE
FULL STORY

The ascent of the bot juggernaut

Nine in 10 firms report that managing bot traffic is challenging.

The rise of bots has rapidly created a minefield for digital business, regardless of their size or geographic location. According to PYMNTS Intelligence data, 89.5% of organizations now report that managing bot traffic is a challenge, with the vast majority characterizing it as “slightly or moderately challenging” or worse. Only a slim minority—barely one in 10 companies—can claim that bot traffic is not a challenge.

This challenge is only going to intensify as artificial intelligence evolves seemingly almost weekly. Over 12 months through September 2025, 52.3% of all surveyed firms reported an increase in bot traffic volume. Fewer than 10% of firms saw traffic levels remain stable.

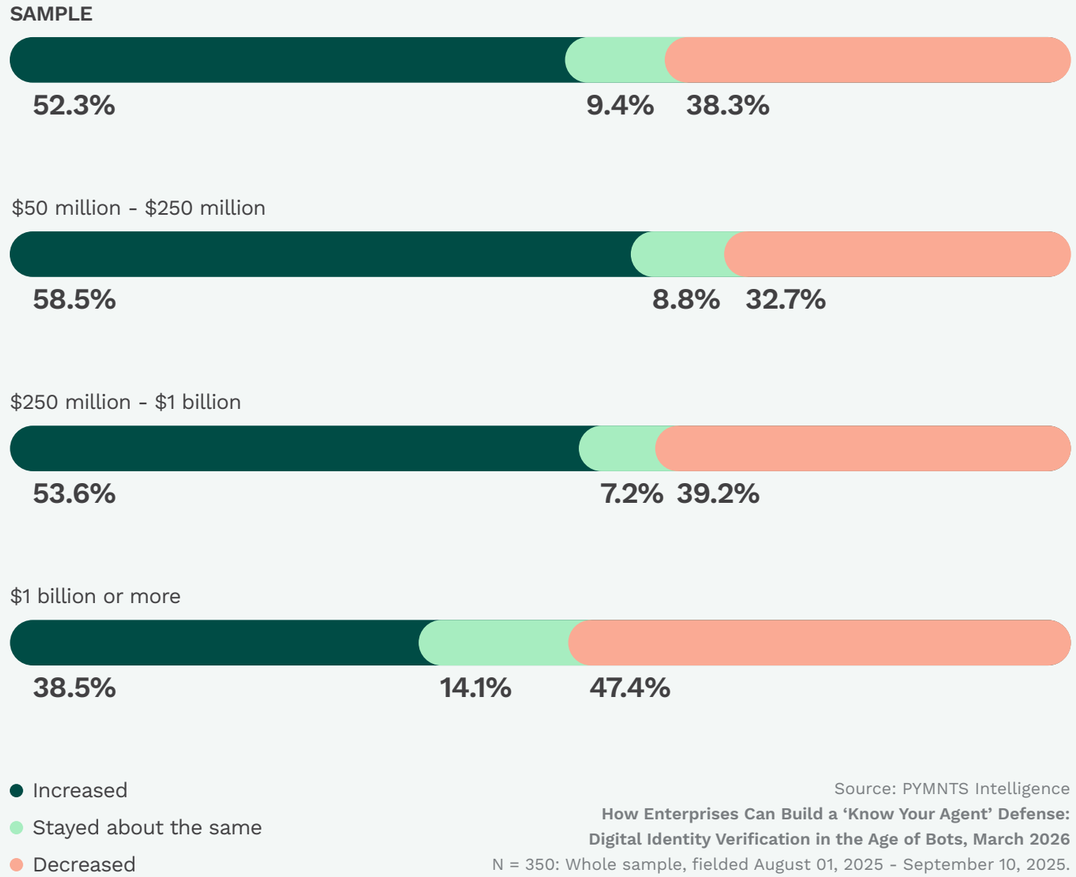
FIGURE 1:

Business impact of bot traffic (past 12 months)

Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

FIGURE 2:

Change in bot traffic over the past year



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

The bigger the company, the greater the attacks and losses

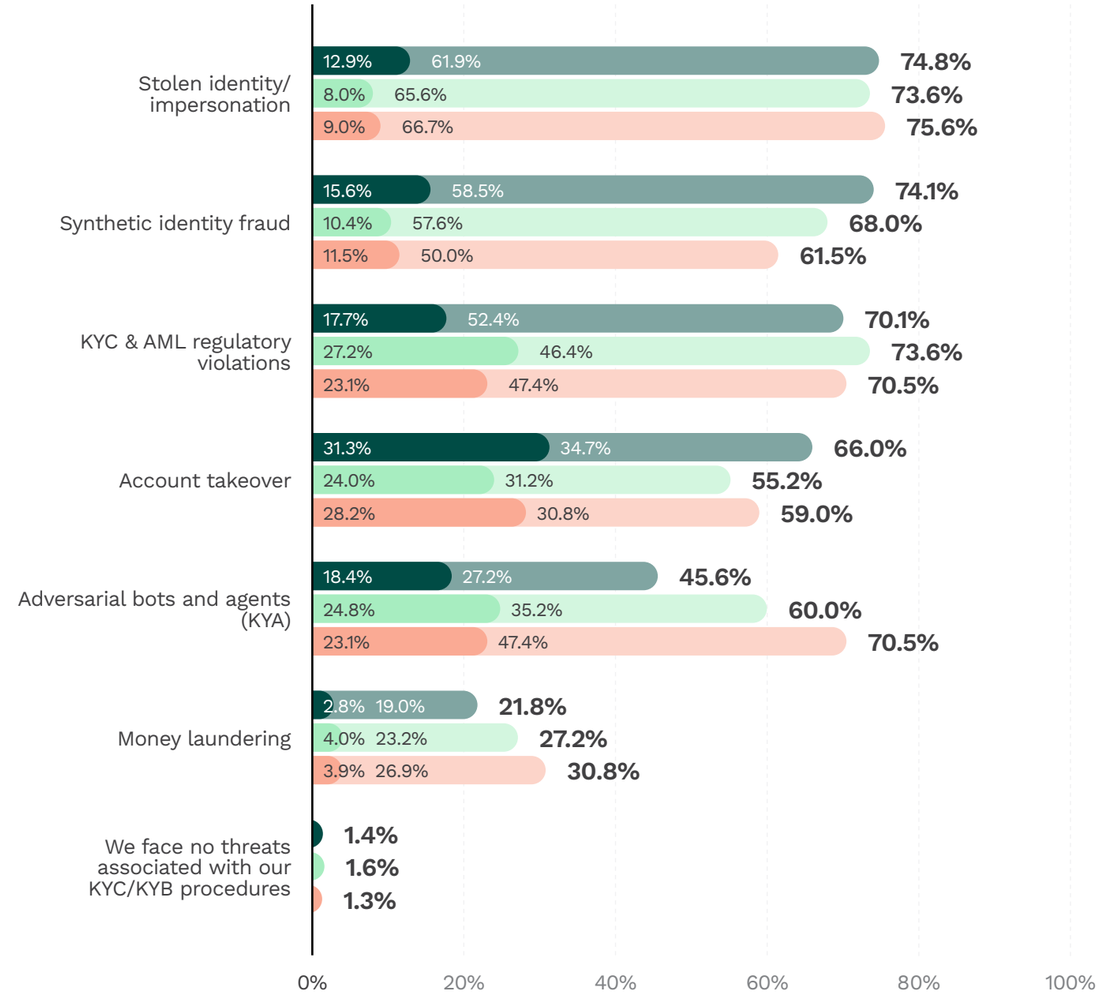
The larger the company, the greater the threat to KYC and KYB processes underpinning KYA.

KYA tools that weed out bad bots depend on strong KYC and KYB processes. As companies grow, identity-driven fraud and sophisticated compliance risks become the primary KYC/KYB challenges, crowding out smaller, lower-impact threat types. Larger firms report a higher rate of every major KYC/KYB threat, and a narrower band of issues accounts for most of their risk.

Smaller firms ($250 million or less in revenue) see a more even spread of problems, with notable but lower levels of stolen identity/impersonation, synthetic identity fraud and KYC/anti-money-laundering (AML) violations. As revenue increases, those same threats become more common and start to dominate the risk picture. Among the largest firms (more than $1 billion in revenue), stolen identity/impersonation and synthetic identity fraud stand out as especially widespread, while traditional issues like basic account takeover and money laundering remain present but relatively less common.

FIGURE 3:

Common and most common threats in KYC/KYB



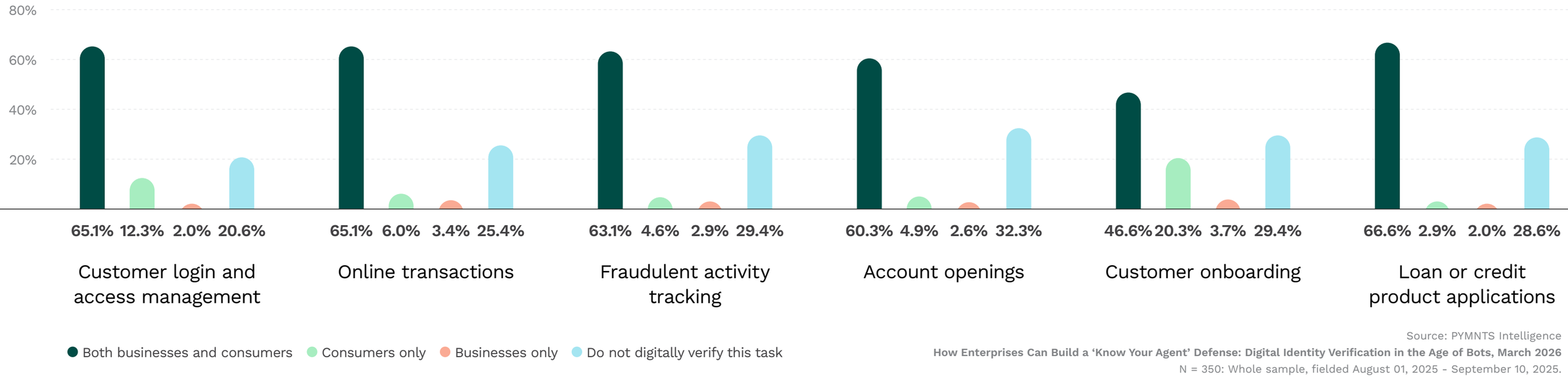
Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

The rise of agentic commerce means that digital identity verification has moved past covering just the account opening stage, the traditional purview of KYC and KYB. Nearly two in three (65.1%) of all firms now apply digital identity verification to customer login and access management. An identical share use it for online transactions. This parity between the “front door” (onboarding) and the “living room” (transactions/logins) shows that security is no longer the domain of a single checkpoint; instead, it requires continuous authentication spanning the entire user lifecycle.

While KYC and KYB verify identity, KYA monitors real-time interactions. **Identity is no longer a one-time check but a continuous surface across all digital touchpoints**, requiring organizations to layer KYA over their existing KYC and KYB processes.

FIGURE 4:

Tasks digitally verified or authenticated via KYC/KYB



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

Credential stuffing and fake accounts hit two-thirds of large enterprises compared to six in 10 with revenues of $250 million to less than $1 billion.

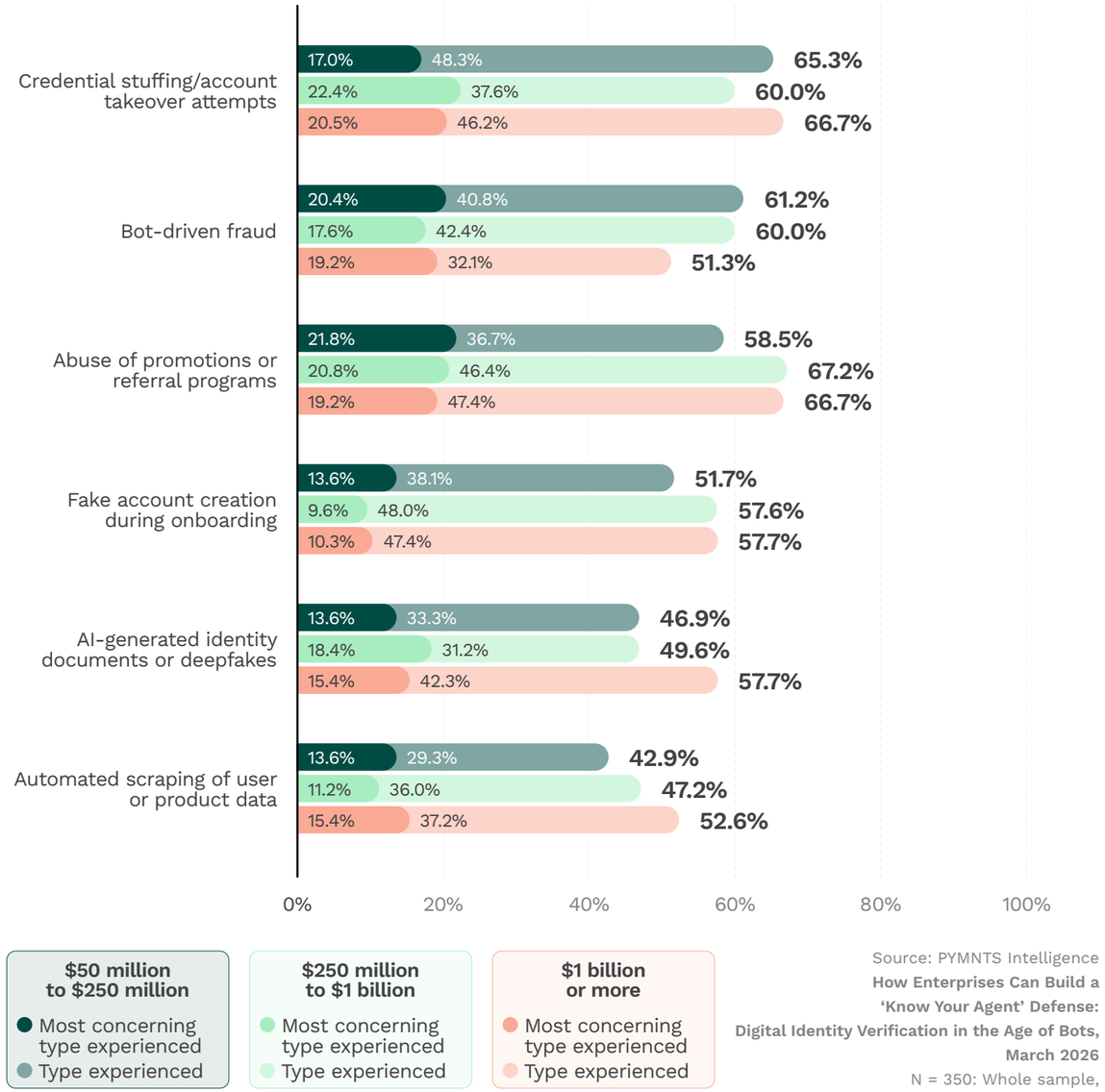
Malicious agents don’t knock once and leave. Firms that run workflows including account opening, fraudulent activity tracking and vendor onboarding consistently report KYA threats. Larger companies in particular face a barrage of industrial-scale attacks that smaller firms encounter far less frequently. These include:

- **Credential stuffing and account takeovers.** Two in three (66.7%) enterprises experience this versus 60% of firms with $250 million but less than $1 billion in revenue.
- **Fake account creation:** Nearly six in 10 (57.7%) battle fake account creation during onboarding, versus 51.7% of smaller firms.
- **AI-generated identity documents or deepfakes:** Nearly six in 10 (56.7%) of enterprises see this, compared to roughly 47% to 50% of companies with revenues under $1 billion.

This data supports the thesis that KYA risk scales not just in magnitude but in the breadth of attack modes firms must manage.

FIGURE 5:

Types and most concerning types of harmful bot activity experienced



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

$1 billion-plus enterprises are nearly twice as likely to have suffered an incident or loss from a bot or automated agent compared to smaller firms.

The conventional wisdom in corporate risk management is that global companies—equipped with nine-figure security budgets, sprawling security operations centers and armies of analysts—are better equipped and protected than their mid-market counterparts. But the data reveals a different reality. In the agent economy, scale acts not as a shield but as a force multiplier for risk. Unlike KYC and KYB, KYA is the only category that scales aggressively with the size of the enterprise.

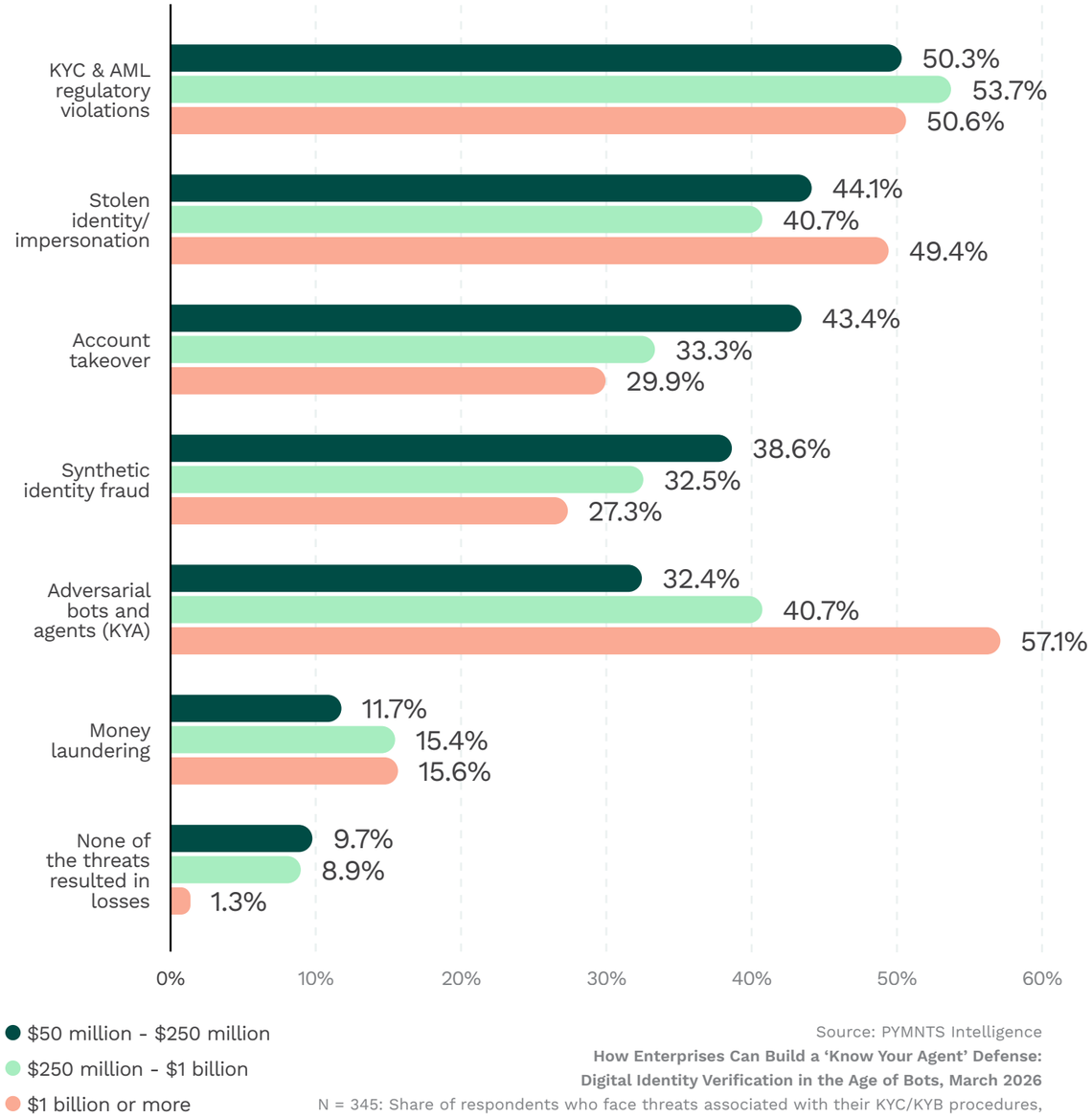
Perhaps most surprisingly, the data shows that loan and credit product applications have become a central theater. Nearly half (48.7%) of all firms report incidents or losses related to adversarial bots and agents in this area, exceeding the damage from stolen identity/impersonation (46.2%) in the same workflow.

As firms grow, the primary vector of concern shifts from the creation of fake identities to the automation of attacks against existing systems. That’s why a modern digital identity framework needs to treat KYA as a scaling layer across KYC and KYB, rather than a standalone risk category.

An organization with at least $1 billion in annual revenues **is nearly twice as likely to have suffered an incident or loss from a bot or automated agent** compared to a company with $50 million to $250 million in annual revenue.

FIGURE 6:

Reported incidents or losses due to identity verification failures



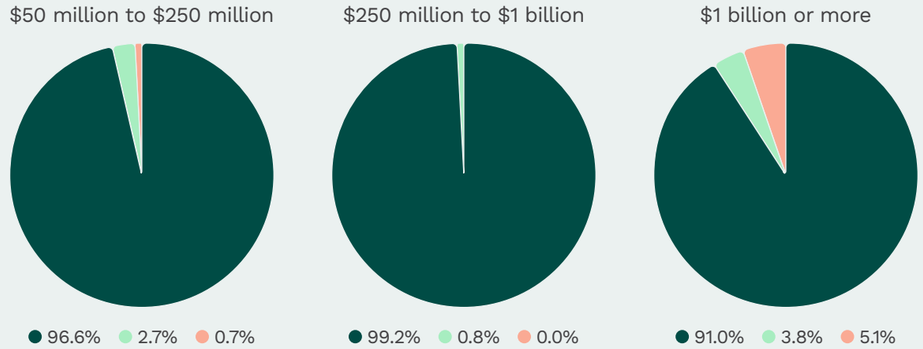
Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 345: Share of respondents who face threats associated with their KYC/KYB procedures, fielded August 01, 2025 - September 10, 2025.

How the ‘good enough’ illusion traps large firms

Despite having the most resources, security leaders at large companies feel the least assured about their digital identity verification systems. Firms with over $1 billion in revenue report a 91% confidence rate, lower than the 99.2% reported by mid-market firms. This may suggest that large enterprises are aware of their exposure. Still, in the agent economy, being a giant doesn’t make you a fortress; it makes you a whale.

FIGURE 7:

Confidence in detecting harmful vs. helpful bots



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

AI industrializes losses due to fraud and missed opportunities

Enterprises with more than $1 billion in revenue or operating in multiple countries report a 3.3% false-positive rate, the most of any type of company.

As organizations scale, they face a dual breakdown in which “good enough” controls fail on both sides of the decision boundary. Large firms are simultaneously becoming too loose (letting in bad actors) and too tight (blocking good customers).

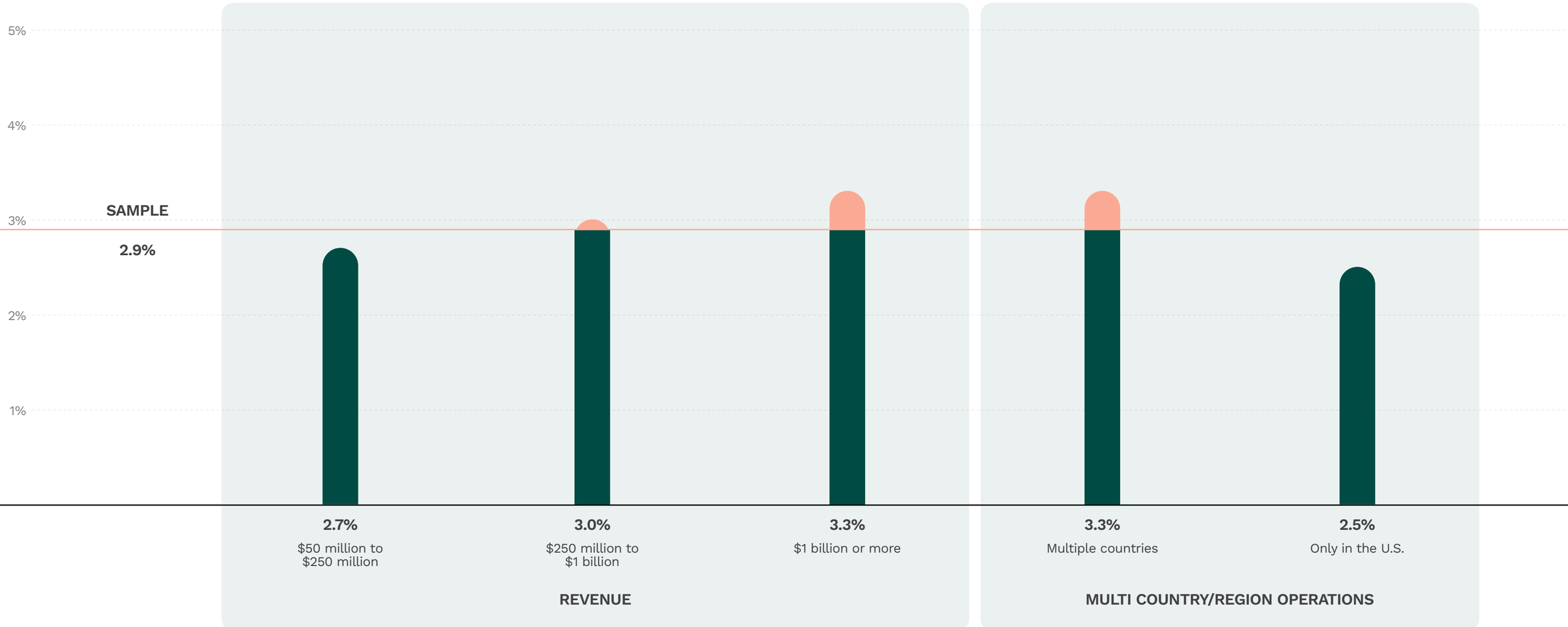
Smaller firms with $50 million to $250 million in annual revenue report an average false-positive rate of 2.7% in digital transactions. For firms with over $1 billion in revenue, the rate climbs to 3.3%. Firms operating in multiple countries report the same 3.3% rate, compared to 2.5% for firms operating only in the U.S.

Nearly two-thirds of enterprises report **losing good customers when they simply give up amid onerous verification hurdles.**

These differences may appear small, but they’re not. At the scale of a global enterprise processing millions of transactions, they represent hundreds of thousands of legitimate customers being blocked, interrogated or annoyed by the system. For $1 billion-plus firms, the perception of false positives as a major friction point jumps from 25.2% to 4%. Nearly two-thirds of enterprises report losing good customers who simply give up amid onerous verification hurdles.

FIGURE 8:

Average false-positive rate in digital transactions



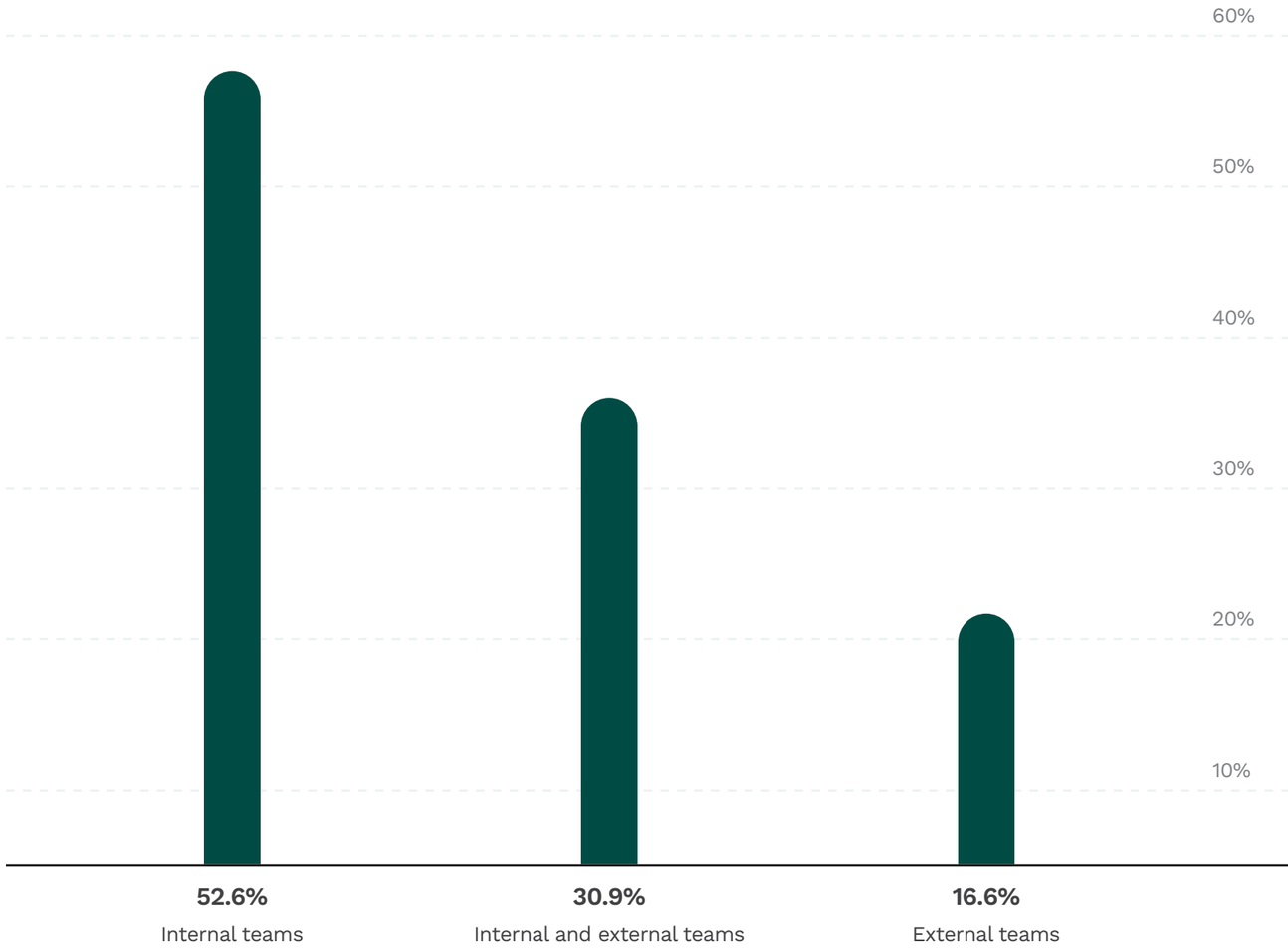
Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

The three operating models of digital identity verification

How a company handles its identity verification systems largely determines the types of attacks they are most vulnerable to.

Just over half of organizations used an in-house system. Only 16.6% use external providers, and the rest deploy a combination of the two.

FIGURE 9:
Primary manager of KYC/KYB operations



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

Here’s how the vulnerabilities of each model break down:

Internal teams are getting hit the hardest by automated threats. They report the highest rate of actual incidents or financial losses driven by bad bots and agents, sitting at 53% compared to just 24.1% for external teams and 28.8% for hybrid models.

82.8%

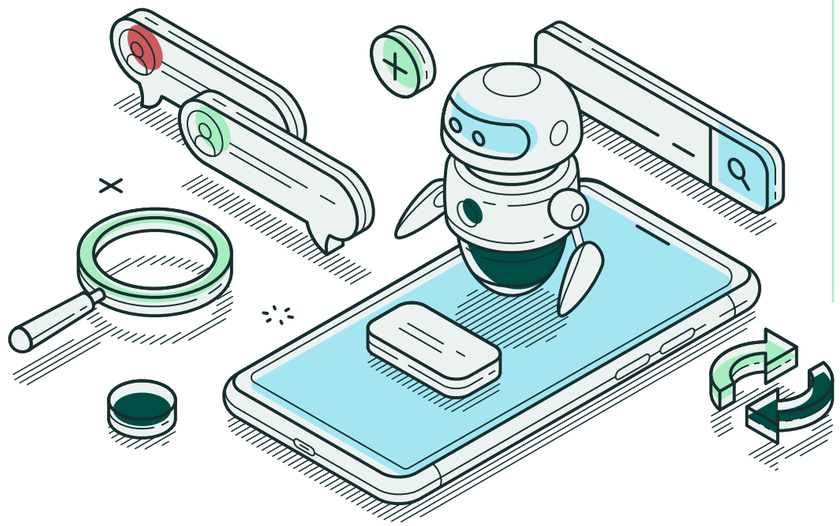
of organizations using third-party identity verification providers **report that their outsourced technology produces frustratingly inconsistent results.**

In-house:

The vulnerability of managing verification in-house largely stems from a reliance on older, manual processes. Because internal teams have low adoption rates for advanced tools like biometric verification (29.3%) and device tracking (28.8%), they are highly exposed to modern, sophisticated attacks like AI-generated deepfakes (64.1%) and automated data scraping (57.6%). Consequently, half of these internal teams admit to accidentally letting untrustworthy suppliers into their systems.

External tools:

Meanwhile, external teams face a unique operational vulnerability. Fully externally managed teams report a much lower 48.3% exposure rate to these attacks. But while they suffer fewer direct losses from bots, 82.8% report that their outsourced technology produces frustratingly inconsistent results.



Hybrid in-house and external tools:

Companies using this two-pronged solution rely heavily on advanced, real-time technologies like biometrics to defend their systems. However, this doesn’t make them immune to vulnerabilities; it just changes the nature of the attacks they face. Hybrid teams, for instance, experience the highest rates of credential stuffing and account takeover attempts (73.1%), as well as fake account creation during the sign-up process (60.2%).

They report a much lower exposure rate of 27.8% to these threats. This stark difference highlights the importance of layered, real-time technology, such as biometric verification and device fingerprinting, in successfully detecting and mitigating sophisticated AI fakes before they bypass human reviewers.

Half of companies managing identity verification in-house say they onboard suppliers they don’t trust.

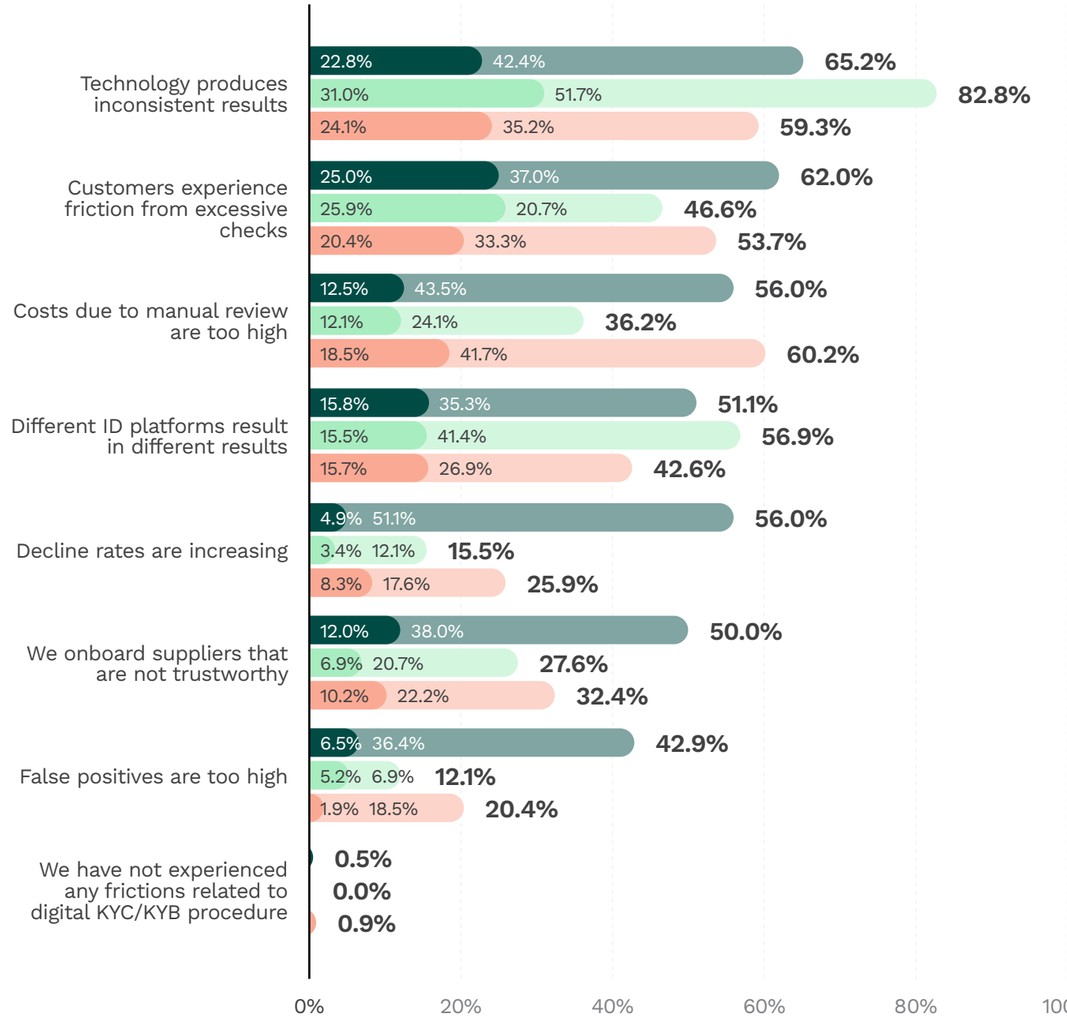
Many firms say that failed KYC/KYB checks create serious headaches for their teams and customers. Internal teams struggle most with inconsistent technology results, customer friction from extra checks, and rising decline rates. These companies are the most likely to onboard untrustworthy suppliers, at 50%, compared with 32.4% for hybrid models and 27.6% for fully external models.

Meanwhile, external teams feel the biggest pain from tech inconsistency and the cost and complexity of managing different ID platforms. They report the highest share of inconsistent identity results, at 82.8%, suggesting that once verification is handed off, coordination gaps and uneven decisions become major failure points.

When internal and external teams share responsibility, they still report high friction from manual-review costs and inconsistent outcomes. About one-third of these firms (32.4%) report they onboard untrustworthy suppliers and nearly six in 10 (59.3%) cite inconsistent identity results as a key friction point. Simply adding more parties does not fix underlying verification issues.

FIGURE 10:

Frictions and biggest frictions from KYC/KYB failures



Source: PYMNTS Intelligence
How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

Identity models drive KYA vulnerabilities and costs

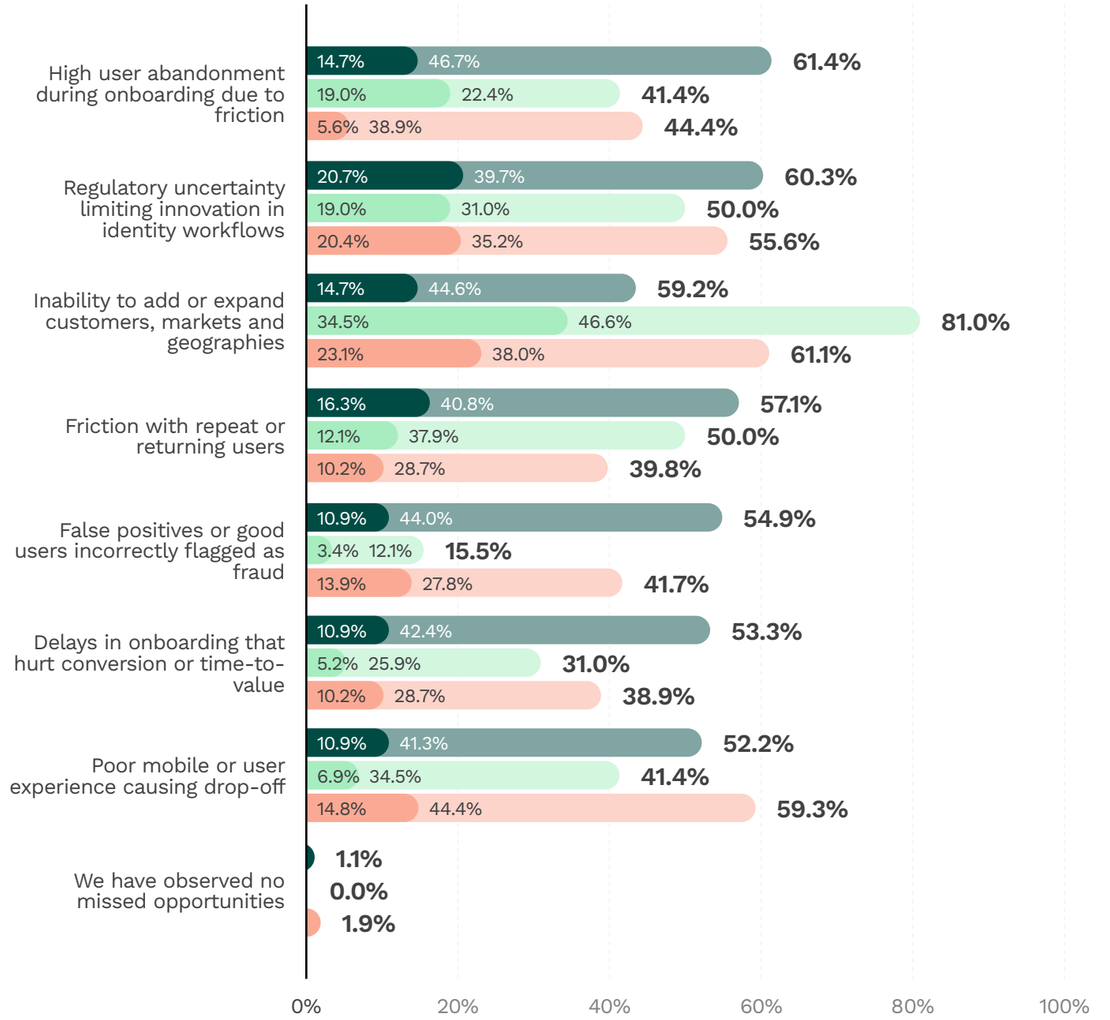
Six in 10 companies that manage identity verification with in-house tools only say they lose customers due to friction during onboarding.

How a company chooses to operate its digital identity verification systems also determines the business impact it faces.

Firms relying on external teams are more likely to report missed growth opportunities, especially an inability to expand into new markets or geographies (81% versus 59% to 61% for internal/hybrid). Internally managed programs more often report customer-side losses, including onboarding abandonment due to friction (61.4% versus 41% to 44%).

FIGURE 11:

Missed and biggest missed business opportunities from KYC/KYB processes



Source: PYMNTS Intelligence
How Enterprises Can Build a 'Know Your Agent' Defense: Digital Identity Verification in the Age of Bots, March 2026
N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

Verifying a business is generally more expensive than verifying a consumer, costing an average $39 compared to $20. Internal teams face the highest direct financial costs per verification check. Because they rely so heavily on manual reviews by their staff (86.4%), their processes are expensive and prone to operational friction.

This creates a massive hidden cost in the form of a 3.3% false-positive rate, meaning they block legitimate, good customers by mistake. Because of this excessive friction, 61.4% of internally managed teams report losing valuable business because frustrated users simply abandon the sign-up process halfway through.

Firms that outsource digital identity verification to external teams enjoy the lowest direct costs per check and the lowest false-positive rate (2.2%). But this comes with a steep strategic cost. An overwhelming 81% of externally managed teams say their setup severely limits their ability to expand into new geographic regions and markets. For these firms, confidence in the reliability of a verification system rests almost entirely on the quality of their vendors (82.8%) rather than their own internal capabilities.

Organizations with mature KYC and KYB capabilities are uniquely positioned to **extend those controls into the agent layer, transforming identity from a vulnerability into a verification system** that builds a strategic advantage with positive economic impact.

Hybrid teams strike a middle ground, with a 2.7% false-positive rate and direct costs that fall securely between the internal and external extremes. Ultimately, businesses must choose their preferred financial trade-off: Internal teams spend more cash and lose customers to frustrating sign-ups, while external teams save money but sacrifice crucial global growth opportunities.

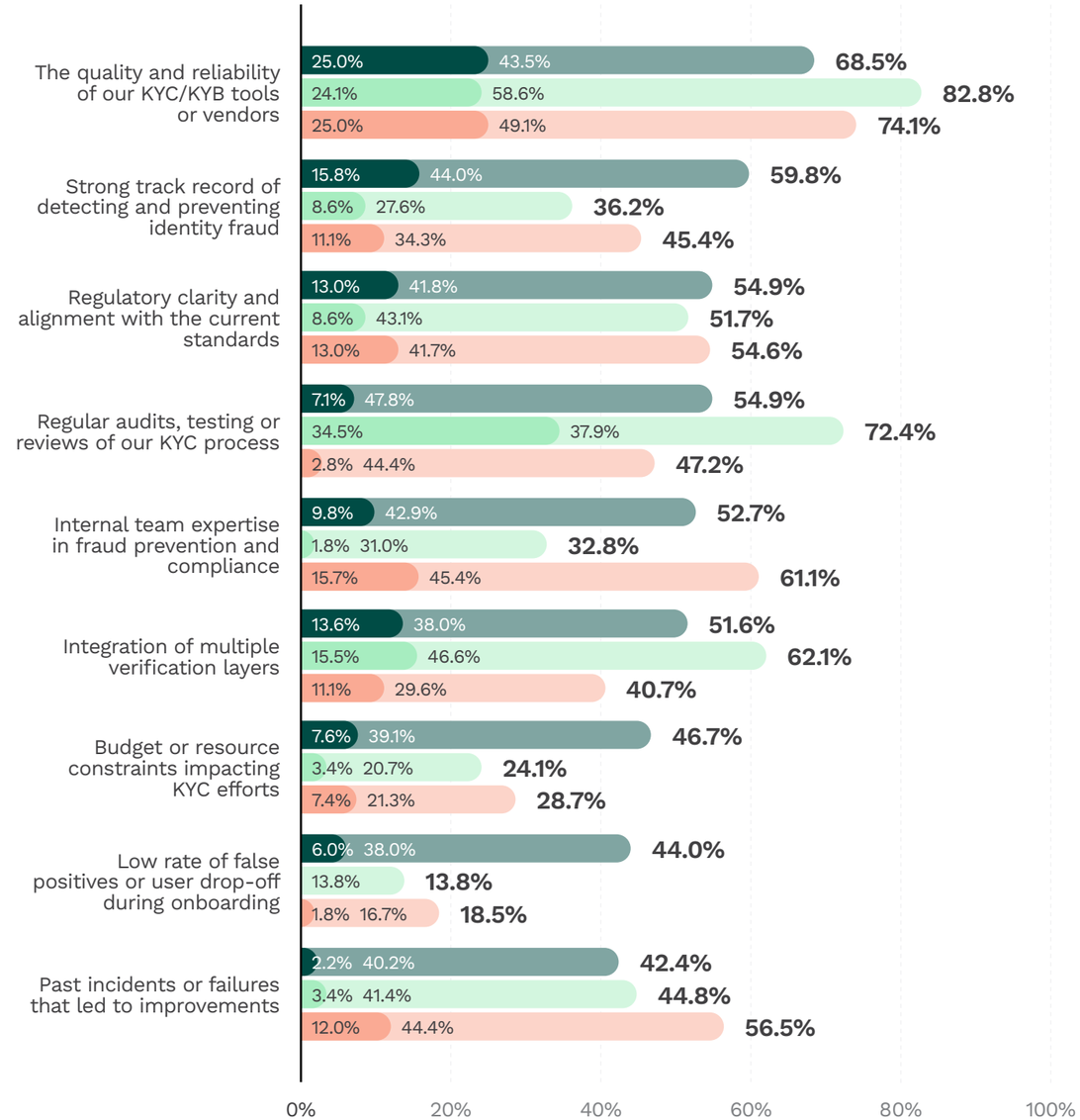
What drives confidence

Across all operating models, the most critical driver of confidence in a digital identity verification system is the quality and reliability of KYC/KYB tools and vendors. This reliance is especially pronounced for firms that fully outsource their operations to external teams. A massive 82.8% of these firms cite vendor quality as a driving factor, compared to 68.5% of internally managed teams.

Beyond simply trusting their vendors, externally managed programs also place a much greater emphasis on structured, multi-layered controls to ensure accuracy. Specifically, 72.4% of external teams rely heavily on regular audits, testing or process reviews. More than six in 10 (62.1%) point to the integration of multiple verification layers as a vital source of their confidence. The takeaway is that as businesses face mounting KYA pressures, their confidence in defending against them is fundamentally tied to the strength of their layered verification tech stack and rigorous, ongoing testing.

FIGURE 12:

Factors and most important factor behind confidence in identity verification



Internal teams
- Most important factor behind confidence in identity verification
- Factors behind confidence in identity verification

External teams
- Most important factor behind confidence in identity verification
- Factors behind confidence in identity verification

Internal and external teams
- Most important factor behind confidence in identity verification
- Factors behind confidence in identity verification

Source: PYMNTS Intelligence

How Enterprises Can Build a 'Know Your Agent' Defense: Digital Identity Verification in the Age of Bots, March 2026

N = 350: Whole sample, fielded August 01, 2025 - September 10, 2025.

The five-layer KYA model

Strong KYA goes beyond traditional tools.

Effectively implementing KYA requires core capabilities across five layers that extend beyond traditional bot detection and fraud prevention. This five-layer model embeds identity checks directly into transaction workflows, rather than treating them as isolated gates.

Principal Verification: KYC validates individual consumers; KYB validates businesses, beneficial owners, and control structures. Any vulnerability here, such as a synthetic or compromised identity, flows directly into the agent layer.

Authorization Binding: Principals grant agents narrowly defined permissions: spending limits, merchant allow lists, product categories, temporal constraints and conditional rules. This layer determines what an agent is allowed to do, not merely that it exists.

Agent Credentialing: Agents receive cryptographic credentials that encode both identity and authorization scope. These credentials must be portable, machine-verifiable and resistant to replay or misuse.

Continuous Trust Validation: Real-time monitoring ensures that authorization remains valid and that the principal’s status has not changed. Revocation, expiration or anomalous activity must immediately constrain agent behavior.

Behavioral Verification: Ongoing analysis evaluates whether agent behavior aligns with expected patterns for its role, permissions and operating context.

KYA Architecture: Five-Layer Dependency Pyramid for Digital Identity

Interlocking security and continuous trust model for FinTech and payments

(Top) **LAYER 5**

BEHAVIORAL VERIFICATION—AGENT PATTERN ANALYSIS
Advanced analytics of agent behavior patterns, machine learning for fraud prediction

LAYER 4

CONTINUOUS TRUST VALIDATION—REAL-TIME MONITORING
Ongoing assessment of agent activity, anomaly detection, dynamic risk scoring

LAYER 3

AGENT CREDENTIALING—AGENTIC TOKENS
Issuing secure, verifiable tokens to authorized agents or devices for autonomous actions

LAYER 2

AUTHORIZED BINDING—CRYPTOGRAPHIC PERMISSION SETTING
Establishing digital permissions, secure key management, linking identity to credentials

(Foundation) **LAYER 1**

KYC/KYB—KNOW YOUR CUSTOMER/BUSINESS
Identity verification, due diligence, legal compliance, foundational data collection

BREACH EFFECT:

CRITICAL FAILURE
Sophisticated threats bypass all defenses, trust is destroyed

COMPROMISES LAYER 5
Malicious activity goes undetected, loss of real-time security, patterns are obscured

COMPROMISES LAYERS 4, 5
Fraudulent agents enter the system, actions become untrusted

COMPROMISES LAYERS 3, 4, 5
Unauthorized access gained, permissions exploited, future actions are invalid

COMPROMISES ENTIRE STACK
Identity foundation is broken, rendering all subsequent layers ineffective

HOLISTIC SECURITY
KYA requires defense-in-depth. A single layer is insufficient; the entire pyramid is required for robust digital identity security.

BREACH PROPAGATION
A successful attack at any level breaks the chain of trust, effectively neutralizing all layers above it, necessitating system-wide reset.

UPWARD DEPENDENCY
Each higher layer relies absolutely on the integrity of all layers below it. There is no trust without a solid foundation.

PYMNTS INTELLIGENCE | Trulioo

ACTIONABLE INSIGHTS

01

Audit and fortify the foundations. Ensure that KYC and KYB processes are rigorous and integrated, as KYA relies entirely on the verified integrity of those elements.

02

Shift from blocking to governing. Move away from binary security models that simply block automation. Instead, build infrastructure designed to welcome authorized agents while excluding adversarial ones, focusing on governing delegated authority rather than just verifying human presence.

03

Integrate identity verification into the full business flow. Stop treating identity verification as a standalone “gate” at onboarding. Embed verification directly into core business workflows, including transaction processing, credit decisioning and supplier onboarding, to prevent trust failures from propagating downstream.

04

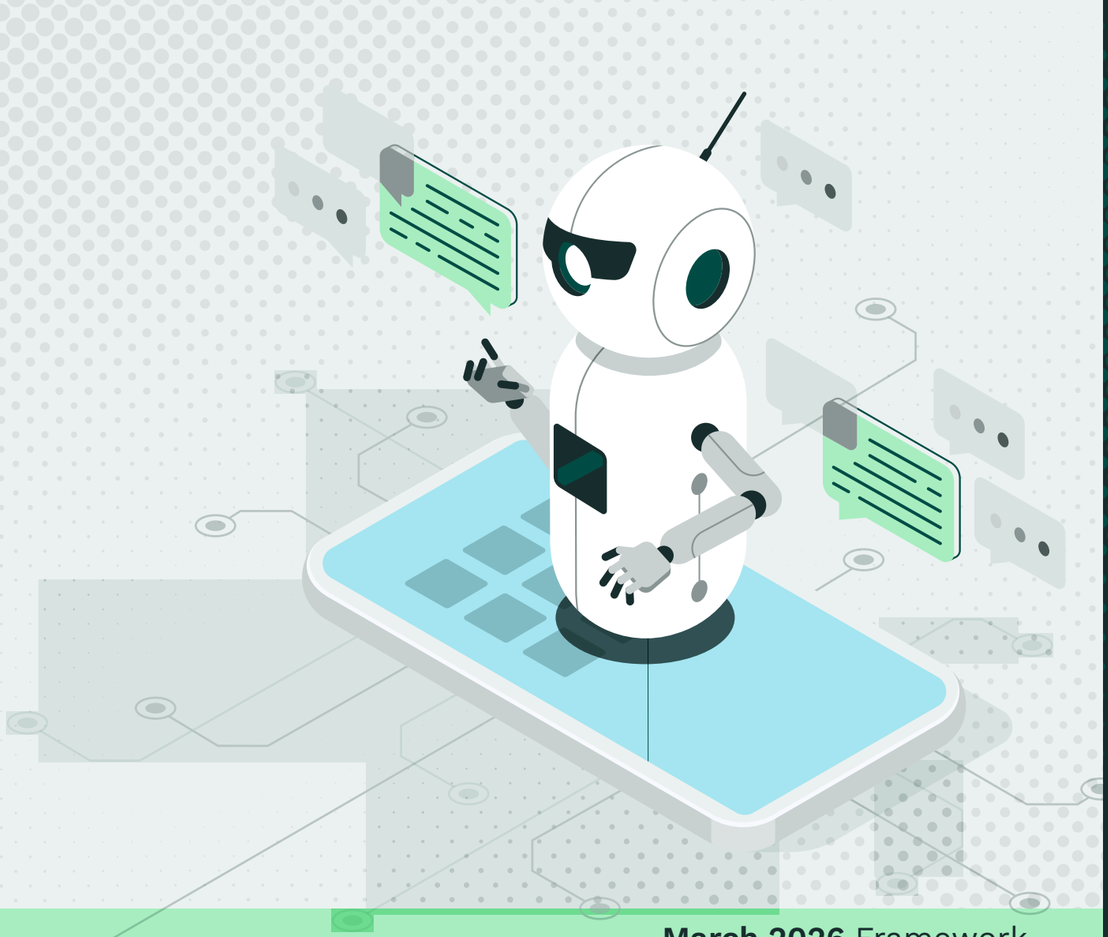
Quantify the total cost of identity verification. Move the budget conversation beyond fraud losses. Calculate and present the full economic impact of the status quo, including customer abandonment ($20M), and operational drag ($5M), to drive investment in modern identity infrastructure.

05

Embrace a hybrid approach. Avoid the pitfalls of purely internal or purely external models. Combine internal policy governance with external platforms that provide global data and adaptive AI to achieve the optimal balance of security and low friction.

06

Adopt the five-layer KYA architecture. Implement a defense-in-depth model that includes principal verification, authorization binding (setting specific permissions), agent credentialing (issuing digital passports), continuous trust validation (real-time monitoring), and behavioral verification (AI-driven anomaly detection).



March 2026 Framework

How Enterprises Can Build a ‘Know Your Agent’ Defense

Digital Identity Verification in the Age of Bots

PYMNTS INTELLIGENCE

Methodology

How Enterprises Can Build a ‘Know Your Agent’ Defense: Digital Identity Verification in the Age of Bots, a PYMNTS Intelligence collaboration with Trulioo, draws on insights from a survey of 350 leaders in compliance, risk management, fraud, underwriting, supplier acquisition and merchant monitoring at global companies that was conducted from Aug. 1, 2025, to Sept. 10, 2025.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT:

Lynnley Browning
Managing Editor

Matthew Albrecht, Ph.D.
Senior Research Analyst

Franco Coraggio
Analyst

ABOUT

PYMNTS INTELLIGENCE

PYMNTS Intelligence is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists include leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues that define the future of the digital transformation of the global economy. This multi-lingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

Trulioo

Trulioo is the world's identity platform, trusted by leading companies for their verification and fraud prevention needs. Offering business and person verification across the globe, Trulioo covers 195 countries and can verify more than 14,000 ID documents and 700 million business entities while checking against more than 6,000 watchlists. Trulioo enables global companies to prevent fraud with hundreds of predictive risk signals, consortium data and industry-specific machine learning models. Its comprehensive suite of in-house capabilities, integrated across a single automated platform, powers customizable onboarding workflows tailored to meet any market requirement. Combining its state-of-the-art technology with expertise across diverse markets, Trulioo enables the highest verification assurance levels, optimizing onboarding costs and fostering trust in the global digital economy.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER

How Enterprises Can Build a 'Know Your Agent' Defense: Digital Identity Verification in the Age of Bots may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.