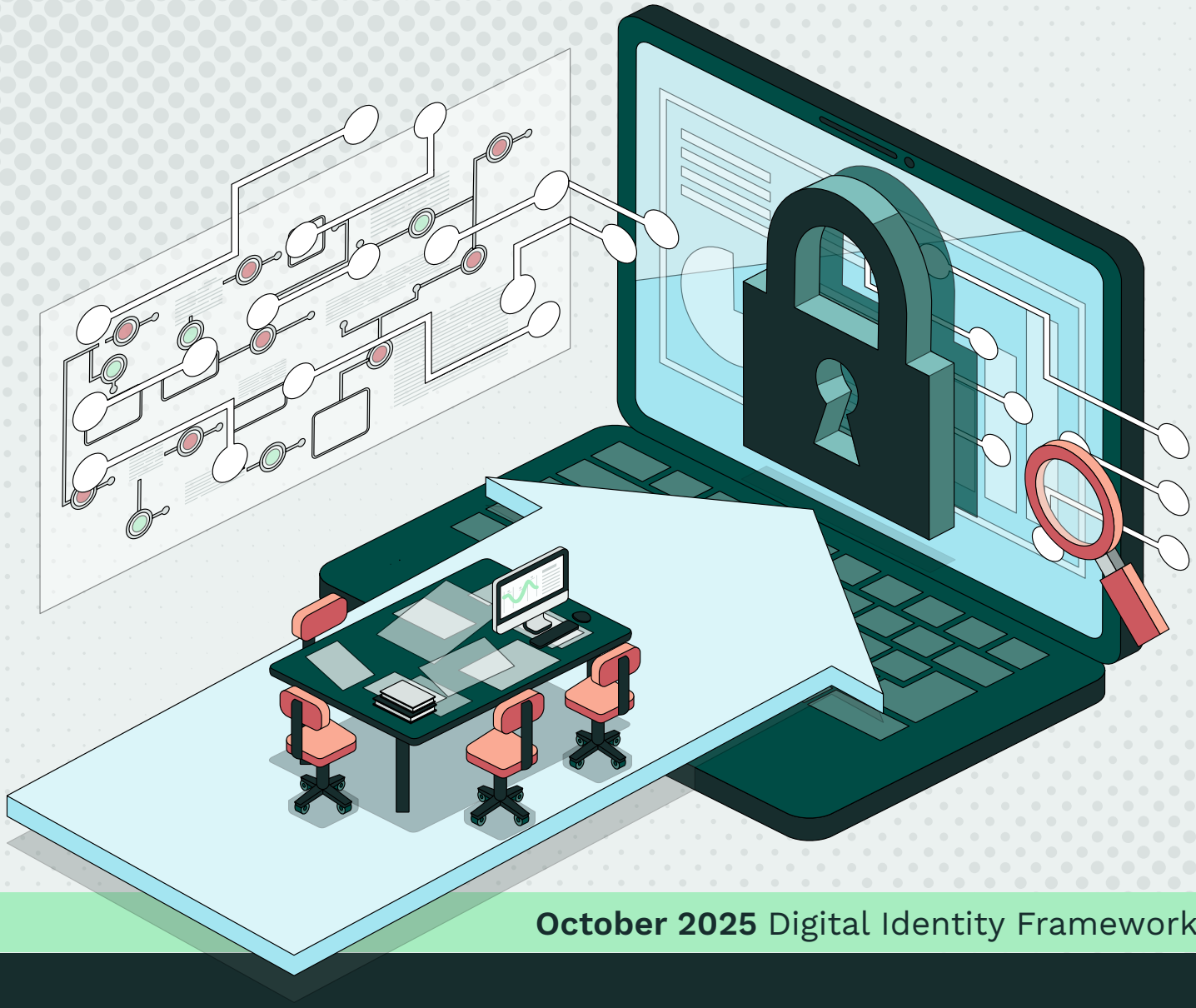


October 2025 Digital Identity Framework

The Hidden Costs of ‘Good Enough’

Identity Verification in the Age of Bots and Agents

PYMNTS INTELLIGENCE | Trulioo

The Hidden Costs of ‘Good Enough’

Table of Contents

PYMNTS INTELLIGENCE | Trulioo

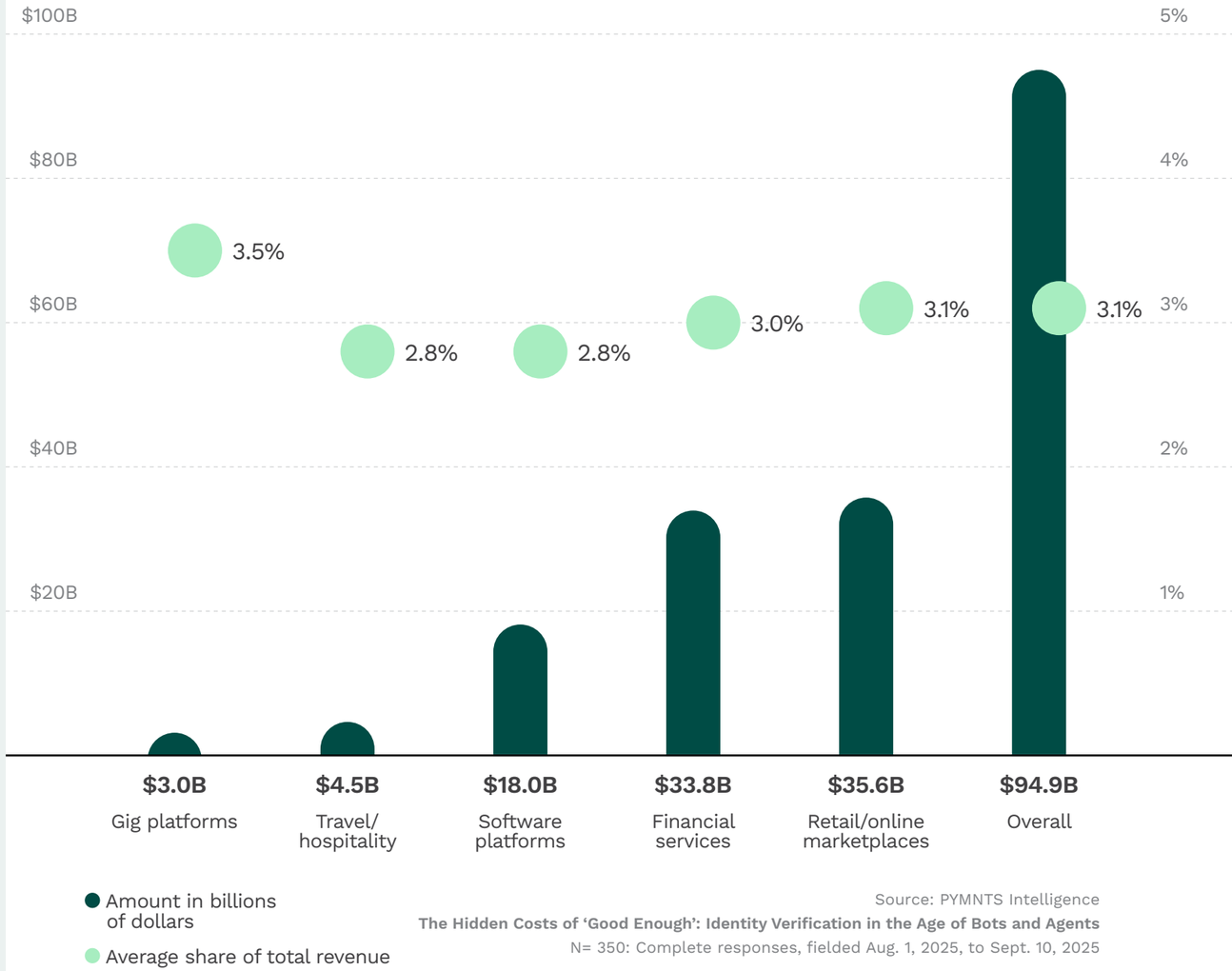
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents was produced in collaboration with Trulioo, and PYMNTS Intelligence is grateful for the company’s support and insight. PYMNTS Intelligence retains full editorial control over the following findings, methodology and data analysis.

What’s **at Stake**

Global companies devote significant resources to software and processes intended to ascertain the identities of consumers and companies they do business with. But even when a digital identity system manages to freeze out fraudsters, it often has an Achilles heel. Many systems wrongly identify valid consumers or suppliers as potential or actual bad actors, a mistake that triggers financial losses when frustrated customers drop out and limits opportunities for market expansion. Companies may also not trust that their current system is capable of onboarding businesses or suppliers that may be new or in other countries.

FIGURE 1:

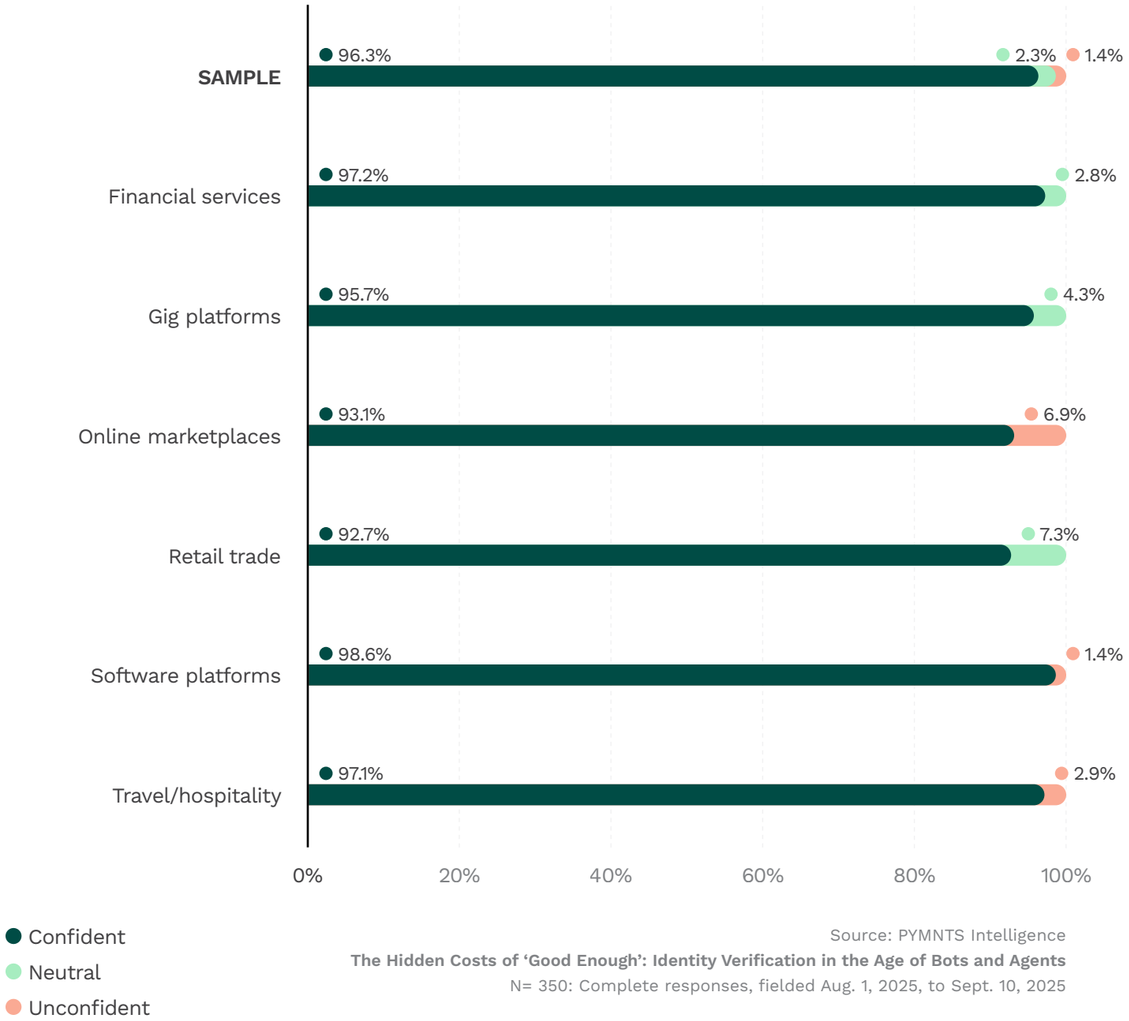
How ‘good enough’ is anything but
Annual revenue loss due to failures in KYC/KYB procedures, by industry



Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

FIGURE 2:

Confidence in detecting harmful versus helpful bots
Share of firms that feel confident in identifying and blocking bad bots



Source: PYMNTS Intelligence
The Hidden Costs of 'Good Enough': Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Whatever the reason, verification lapses are extremely costly. Collectively, firms lose an average 3.1% of annual revenue due to gaps in identifying bad actors, misidentification of legitimate ones and regulatory and compliance breaches resulting in monetary fines. For the 350 respondents in this report, that equates to a collective $95 billion, each year. Digital identification failures don't just add costs—they cost business and block growth.

Despite increasingly sophisticated authentication challenges, nearly all (96%) surveyed companies claim confidence in their ability to detect harmful bots. At the same time, nine in 10 report challenges from harmful bot traffic, and 59% struggle against bot-driven fraud. This disconnect suggests that companies are unaware of the bottom-line cost of having outdated or weak digital identity systems. Despite rapidly evolving digital threats like synthetic identities, account takeovers and cross-platform scams, companies appear to think their systems are "good enough." But even as the "hidden tax" of this misplaced mindset translates into lost cash, fleeing customers and dented trust, it also signals an opportunity. Digital identity systems that function not just as a cost center but as a strategic capability can drive customer conversion, improve customer experiences and strengthen long-term relationships with consumers and suppliers.

3.1%

Average U.S. dollar revenue a company loses each year due to having an inadequate digital identity system

These are some of the findings explored in “The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents,” a PYMNTS Intelligence report in collaboration with Trulioo. The report draws on insights from a survey of 350 global companies conducted from Aug. 1, 2025, to Sept. 10, 2025. Twenty-two percent of companies had annual revenues of at least $1 billion; 36% had revenues of $250 million to less than $1 billion; and 42% had revenues of $50 million to less than $250 million. Industries surveyed included financial services, gig platforms, online marketplaces, retail trade, software platforms, and travel and hospitality. Companies operate in the United States, Canada, U.K., European Union and other European countries, China, India, Japan and other Asia-Pacific countries, the Middle East, Australia/New Zealand, Africa, and Mexico and other Latin American countries.

This is what we learned.

Key Findings

01

Identity failures cost companies customers and cash.

The majority of global companies face threats from adversarial bots and agents, while 1 in 2 report bad customer experiences and high manual review costs.

56%

of companies report threats from adversarial bots and agents.

02

Identity gaps block growth and drain revenue.

Nearly two-thirds of global companies say that weak know-your-customer (KYC) and know-your-business (KYB) processes curb their ability to win new business and expand, with more than half losing potential customers to identification failures.

52.9%

of companies report user drop-off during onboarding, with 44% struggling with false positives.

03

Overconfidence masks vulnerabilities and missed opportunities.

Nine in 10 global companies report challenges from harmful bot traffic, with 59% struggling against bot-driven fraud. Yet 96% claim they’re doing a good job detecting harmful bots.

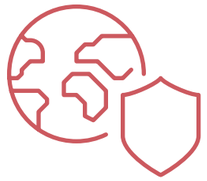
58.6%

of businesses struggle with bot-fueled fraud, with 1 in 5 listing fraud as their top bot concern, above account takeovers, abuses of promotions and referrals, fake accounts, deep fakes and data scraping.

04

Global identity platforms deliver more confidence and better outcomes.

Companies using global platforms to determine the digital identity of their customers report greater confidence in verification quality, more clarity and efficiency, and lower drop-out rates and false positives.



79%

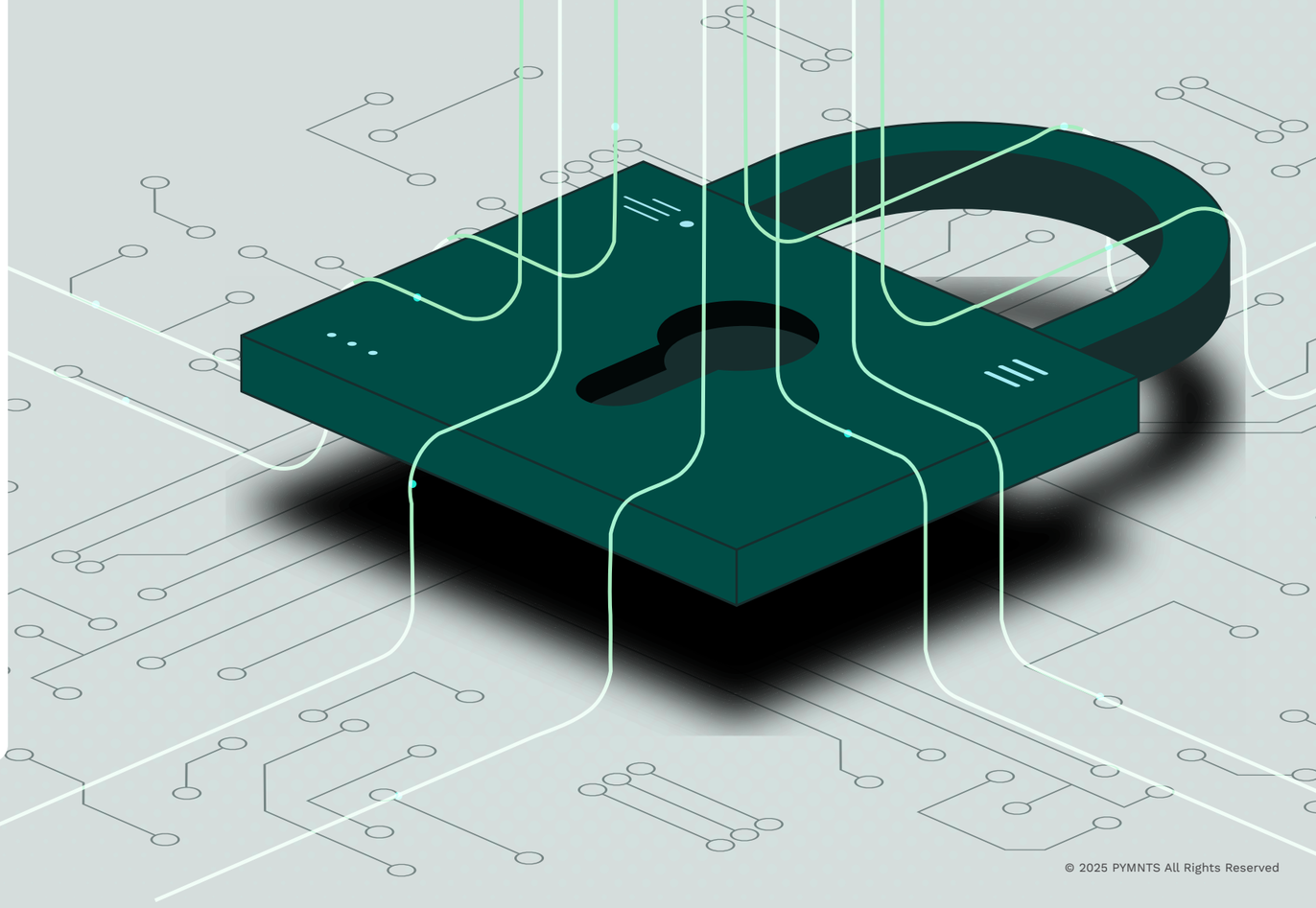
of companies using global identity platforms cite the vendor’s quality and reliability as driving confidence in their verification procedures.

05

An identity edge delivers a competitive advantage.

83.4%

More than eight in 10 companies using a global identity platform rate their system as high performing, while nearly 94% say global identity platforms make KYC/KYB management easier over time.



PYMNTS INTELLIGENCE | Trulioo

PYMNTS
IN DEPTH

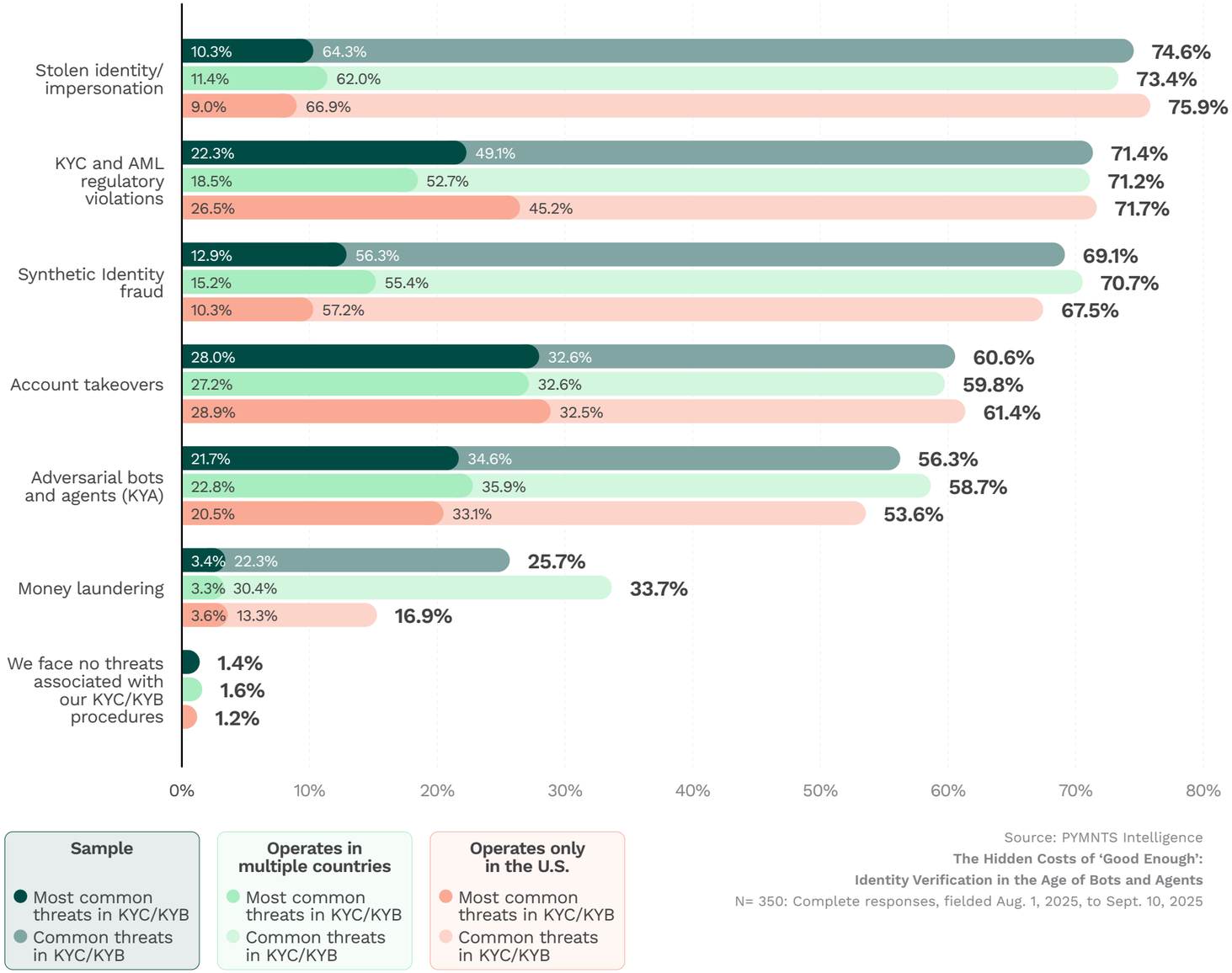
Over half (56.3%) of surveyed companies say they now face threats tied to bots or agents.

KYC verification tools center on consumers and are intended to protect against stolen identities, customer impersonation, money laundering, breaches of anti-money laundering rules, synthetic identity fraud (when scammers combine invented credentials with legitimate ones tied to a real person) and account takeovers. False declines, which is when legitimate consumers are labeled as problematic, are a major shortcoming of inadequate digital identity systems.

KYB tools center on suppliers and are intended to protect companies from accidentally onboarding unscrupulous ones. But they also have an Achilles heel: An inadequate KYB system can cause a company not to expand into new markets. The reason: The company doesn’t trust that its system is capable of onboarding legitimate businesses or suppliers that may be new or in another country.

FIGURE 3:

Threats that are either frequent or the most common for KYC/KYB processes



Source: PYMNTS Intelligence
The Hidden Costs of 'Good Enough': Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Both sets of identity verification and authentication tools function as a defense against fraud, liability and breaches of regulatory compliance requirements. But identity is no longer just about verifying who someone is—it's about determining what someone is (malicious bot or legitimate human/business), and in a way that reduces friction and unlocks growth. A recent white paper co-written by Trulioo and PayOS details how for merchants, issuers, processors and regulators, it's imperative to Know Your Agent (KYA).

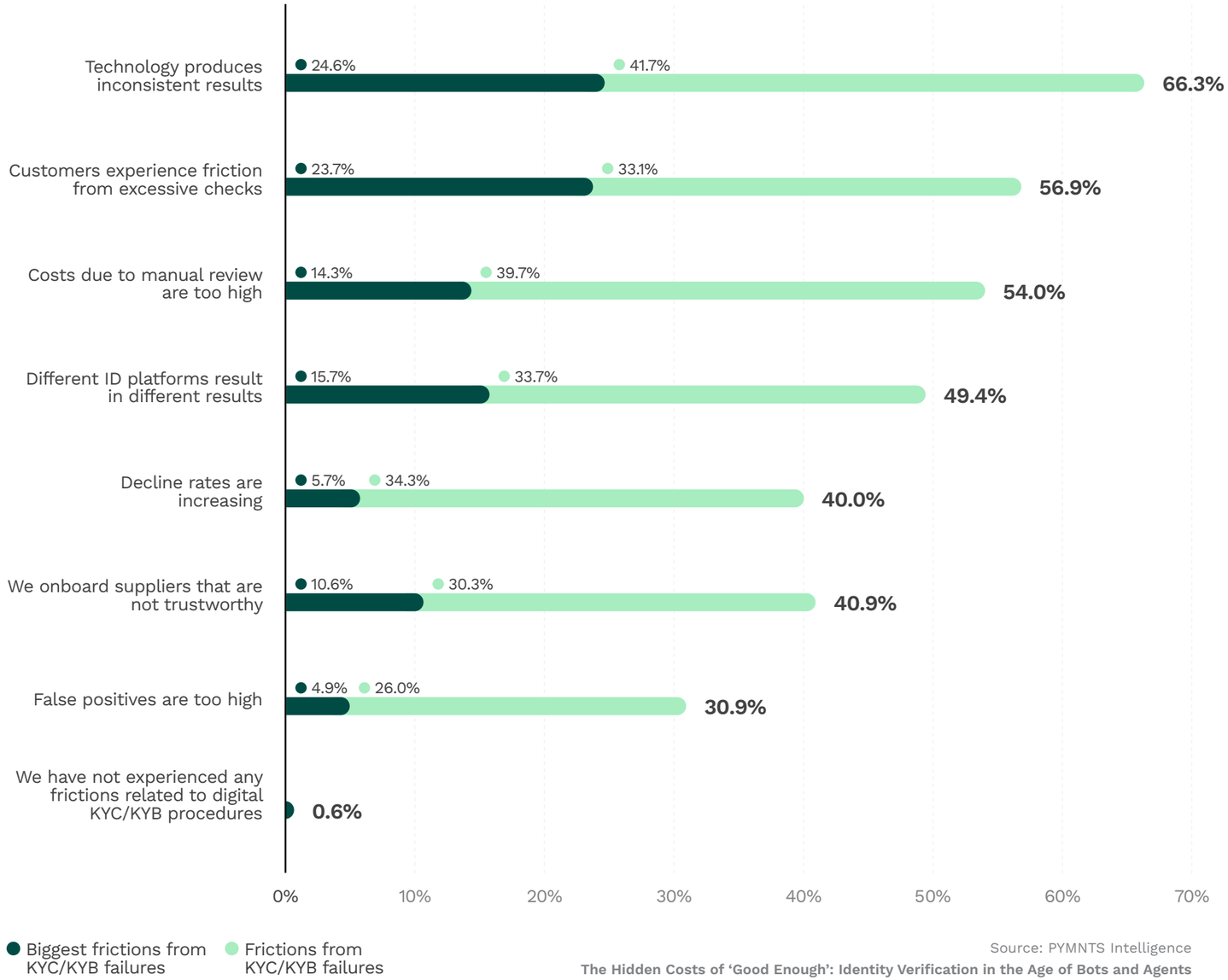
Over half (56.3%) of surveyed companies say they now face threats tied to bots or agents. More than one in five businesses say the use of those AI-fueled tools to commit fraud is their top threat, underscoring heightened risks for their operations and compliance. As the AI-driven threat landscape evolves, companies with robust global digital identity systems are better equipped to tackle malicious bots and agents and move from surviving in the AI-driven economy and its rapid changes to thriving.

One in two companies report that gaps in their identity verification systems result in poor customer experience, excessive digital checks that annoy and drive away potential customers, false positives (where a customer is mistakenly flagged as suspicious), or inconsistent results that sometimes get things right, other times, wrong. These companies also face high manual review costs, underscoring how digital identity inefficiency is a systemic issue affecting firm-wide operations. Each time a legitimate customer encounters friction, there’s a hidden cost: lost revenue, wasted resources and customer attrition.

What’s more, many digital identity systems increasingly miscategorize legitimate customers. Four in 10 companies say their decline rates (when onboarding a new customer or supplier) are rising, a trend that is likely erroneously turning away at least some good business. Strikingly, just as many companies report onboarding suppliers they don’t deem trustworthy. It’s possible that’s an outcome of global companies adjusting their supply chains on the fly to cope with tariffs.

FIGURE 4:

Frictions that are either frequent or the most common in KYC/KYB failures



Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

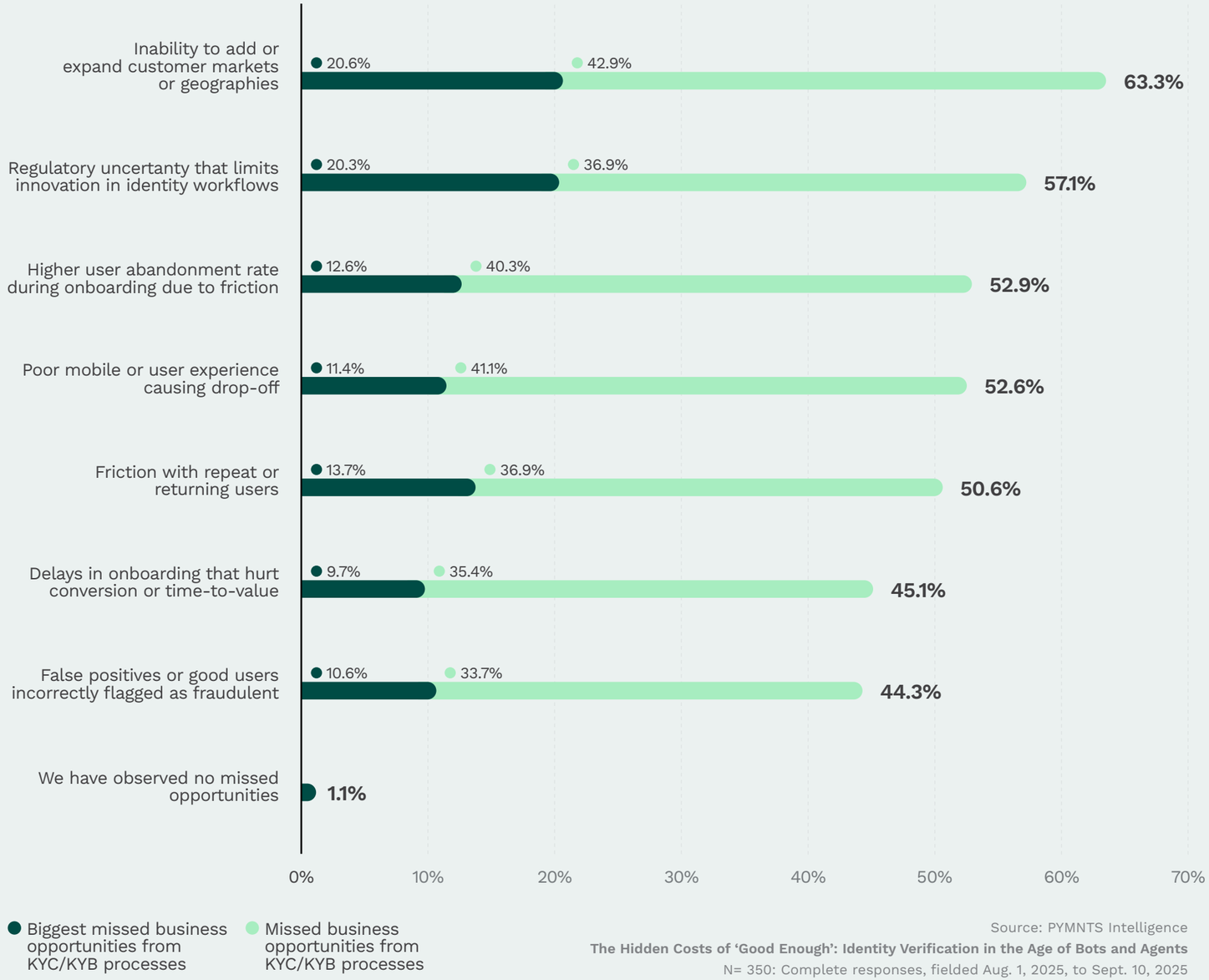
Identity gaps needlessly stymie corporate growth and cost on average 3.1% of annual revenue.

KYC and KYB processes have long been the workhorse of processes aimed at ferreting out and stymying fraudulent transactions by consumers, business customers and suppliers. But they’re not fully working. Nearly two-thirds of companies (63%) say that gaps in these processes limit their ability to expand into new markets and gain new customers. More than half lose customers to onboarding drop-offs due to friction. Over four in 10 (44%) struggle with false positives that mistakenly flag legitimate customers as illicit.

Whether it’s due to actual fraud that a digital identity system fails to detect or to mislabeling a good customer as suspicious, the cost of these failures is substantial: 3.1% of annual revenue.

FIGURE 5:

Missed business opportunities that are either frequent or the biggest in KYC/KYB processes



Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

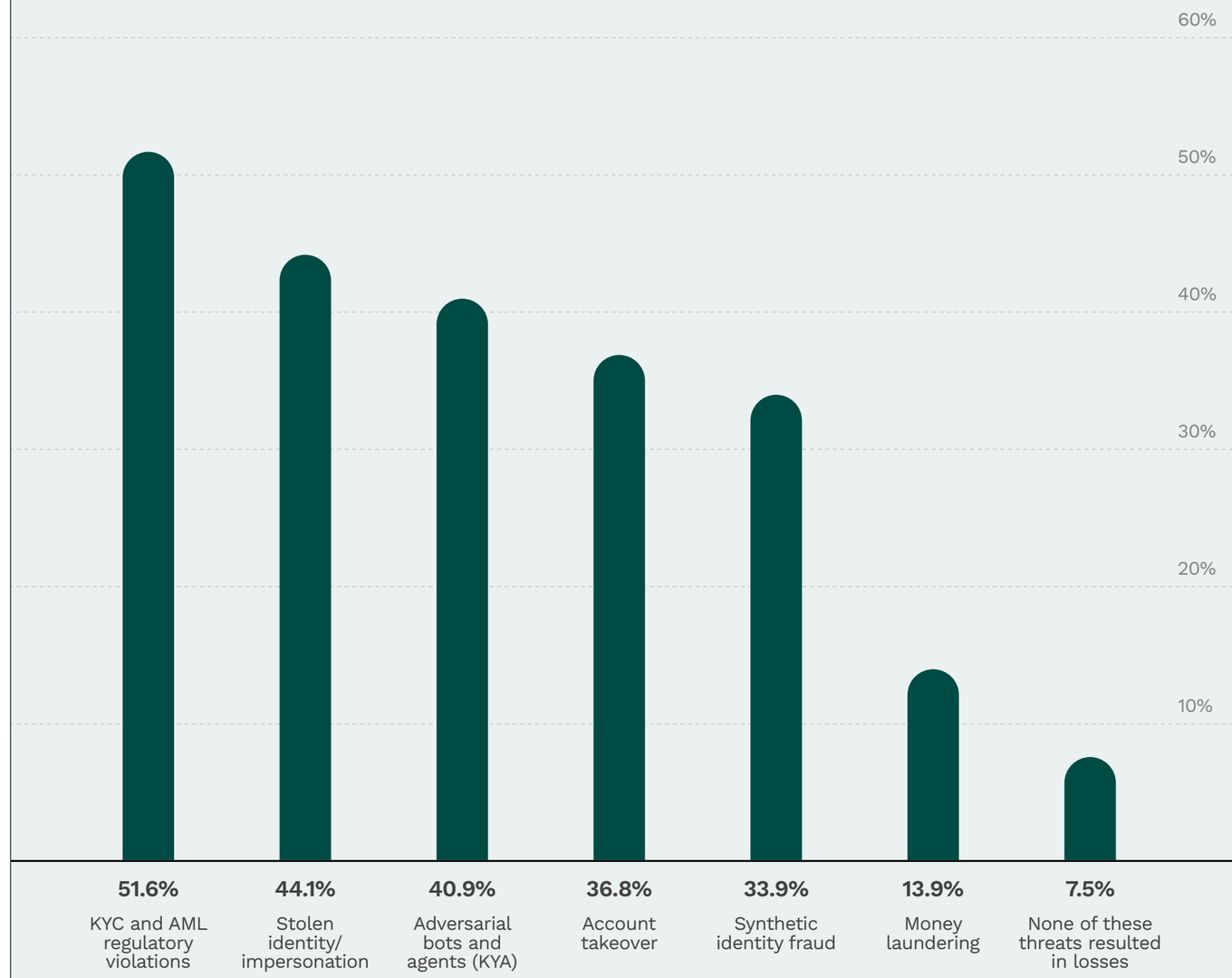
The Hidden Tax of a ‘Good Enough’ Identity

Identity is at the front door of every digital interaction, determining whether a consumer can open an account, whether a gig worker can join a platform, whether a merchant can receive payments and whether a cross-border transaction can be authorized. When an adversarial bot or agent breaches the system, the costs pile up. More than four in 10 companies have experienced losses or incidents related to adversarial bots and agents. That KYA failure rate is close to the 51.6% of companies reporting violation of KYC and AML regulations and 44.1% reporting stolen identities or impersonation of legitimate customers.

Added up, these failures and costs can be thought of as the “hidden tax” for using a digital identity system that seems “good enough.” This mistaken approach is costing companies revenue, limiting growth and hindering customer experience, and it’s increasingly a liability. A recent PYMNTS report on agentic AI found that one-third of U.S. consumers have used or would use generative AI for shopping. With identity and payments converging, regardless of whether a consumer is shopping online, booking travel or paying bills, or whether a business is negotiating supply contracts, “good enough” is a roadblock to reducing fraud, accelerating onboarding, expanding globally and preparing for the age of agent-to-agent transactions.

FIGURE 6:

Reported incidents or losses due to identity verification failures



Source: PYMNTS Intelligence

The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents

N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Adversarial bots exploit every weak point in a digital identity system and turn gaps into an open door.

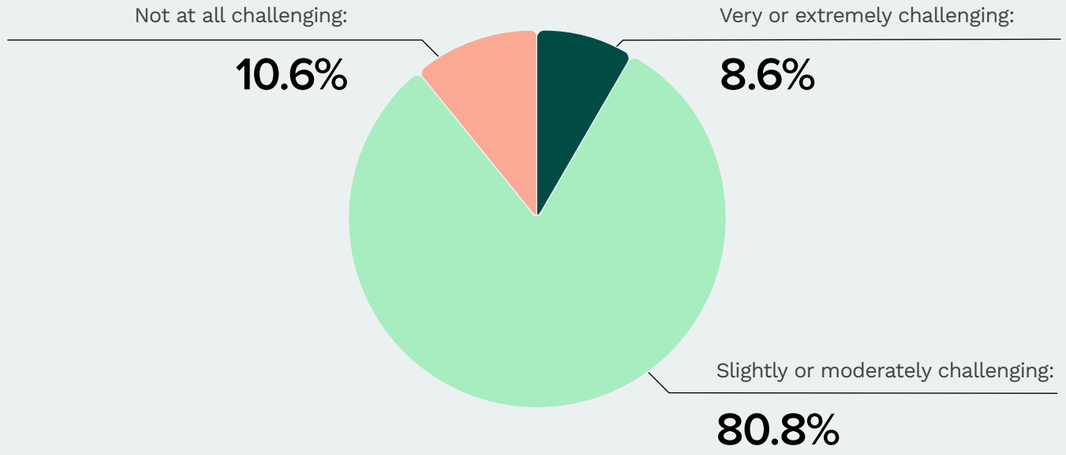
Artificial intelligence gives fraud an expanded market. On average, 59% of firms battle bot-driven fraud. Companies that operate solely in the U.S. are more likely than those in other or multiple jurisdictions to find this a challenge, at just over six in 10 (60.8%).

Nine in 10 companies report challenges stemming from harmful bot traffic. The situation is getting more difficult, with more than one in two businesses reporting rising bot traffic.

Malicious bots can wreak all manner of havoc, from “cart jacking” that falsely makes items appear out of stock to using stolen credentials to hijack user accounts and steal stored payment methods or loyalty points. They can also gain access to order manifests, invoices and shipping updates to intercept or reroute purchased goods.

FIGURE 7:

Impact of bot traffic on business in the last 12 months

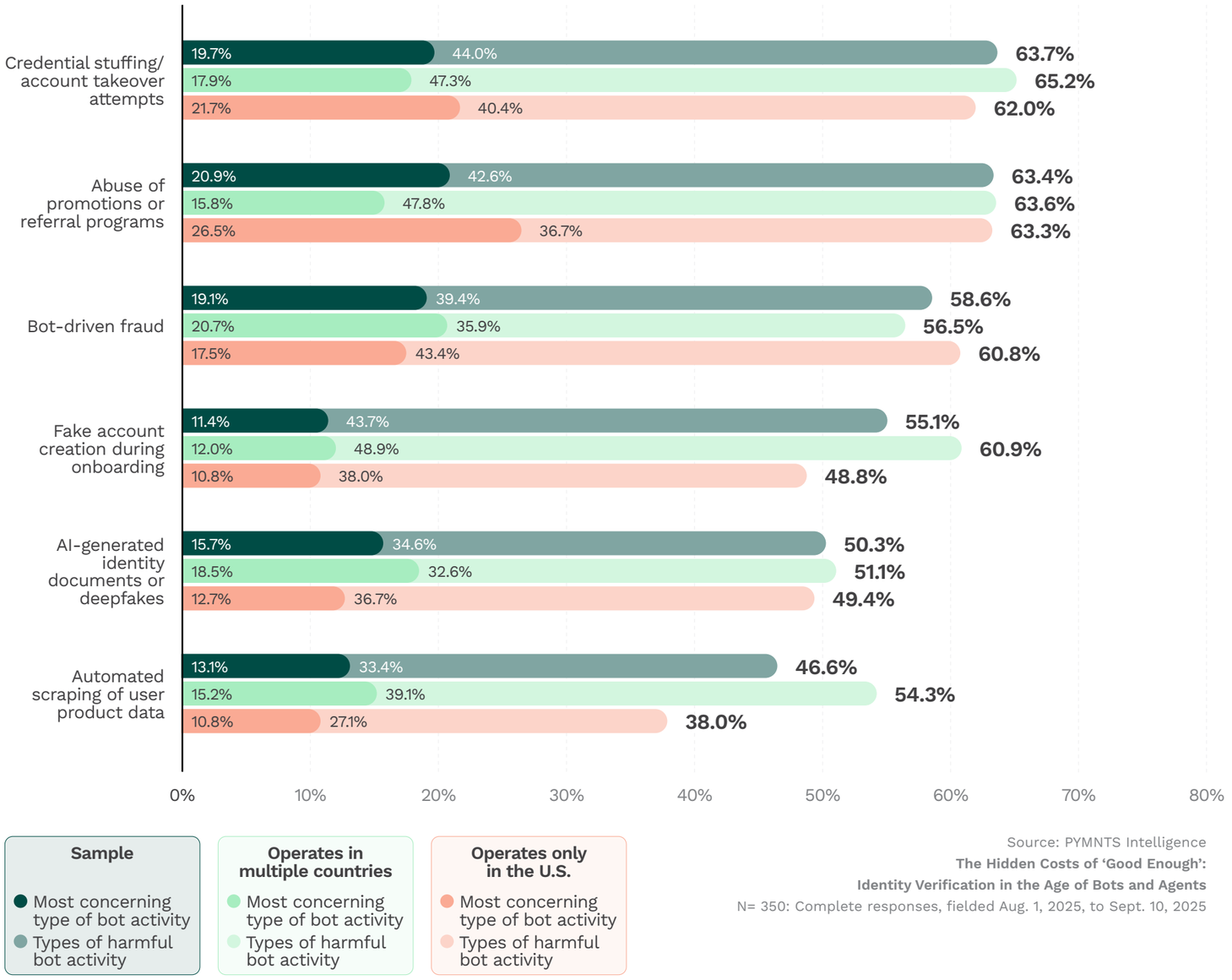


Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

One in five companies peg fraud as their top bot concern. As digital identity expands from regulatory checkpoint to protection of the digital commerce gateway, businesses can no longer treat bots as background noise. Credential stuffing, fake accounts and deepfakes aren’t just fraud issues—they’re systemic business challenges that fuel losses, create friction and undermine customer trust.

FIGURE 8:

Types of harmful bot activity experienced and most concerning types



Source: PYMNTS Intelligence
The Hidden Costs of 'Good Enough': Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

20.9%

of companies cite abuse of **promotions or referral programs as the most harmful bot activity** they face.

Overconfidence in beating bots masks critical weak spots, with over half of firms fighting a rise in bot traffic.

Despite almost six in 10 companies saying they find it tough to get a handle on bot-driven fraud, nearly all (96.3%) say they’re confident in their ability to distinguish harmful bots from helpful ones.

That firms feel secure in their ability to block bad bots even as they report rising fraud levels rise exposes not just the inadequacy of their defenses, but also a blind spot in management strategies. There are two possible reasons for this: Companies may be unaware of the average 3.1% hit to annual revenue that results from having a “good enough” digital identity system. Or they may see fraud as the cost of doing business. Either way, the disconnect between perceived capabilities and actual bottom-line impact exposes a major fault line in many firms’ approaches to managing digital identities.

60.6%

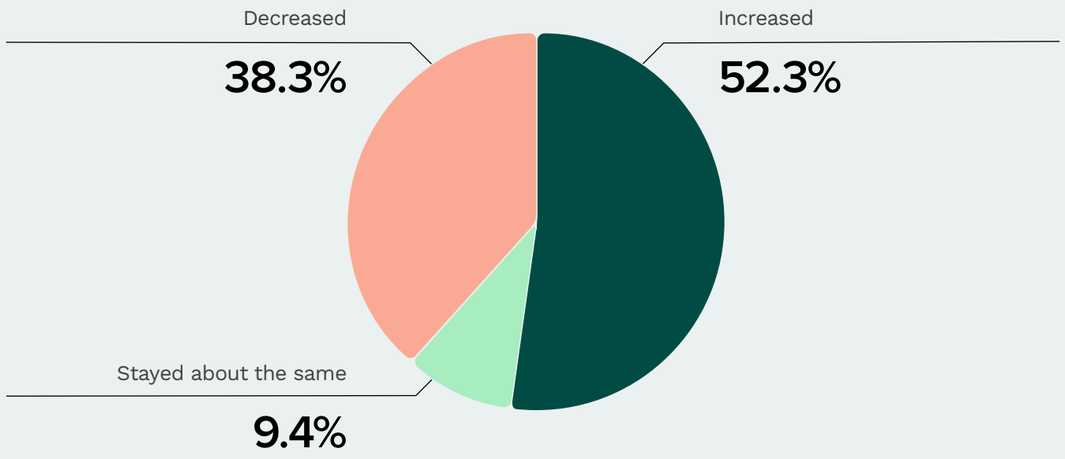
of financial services firms have experienced increased bot traffic in the last 12 months, the most of any industry.

Travel and hospitality firms are at 59.4%, while online marketplaces are at 34.5%.

With more than one in two firms reporting rising bot traffic, the ability to separate bad actors from goods ones is critical. But a defensive stance alone isn’t enough. Fraudsters innovate quickly, tweaking their methods as soon as new defenses are deployed. At the same time, as companies largely focus on stopping harmful bots, they can overlook the growth of helpful ones and the business opportunities they present. The data indicate that the ability to separate harmful from helpful bots is critical, and defense alone isn’t enough.

FIGURE 9:

Companies’ reported changes in bot traffic over the past 12 months

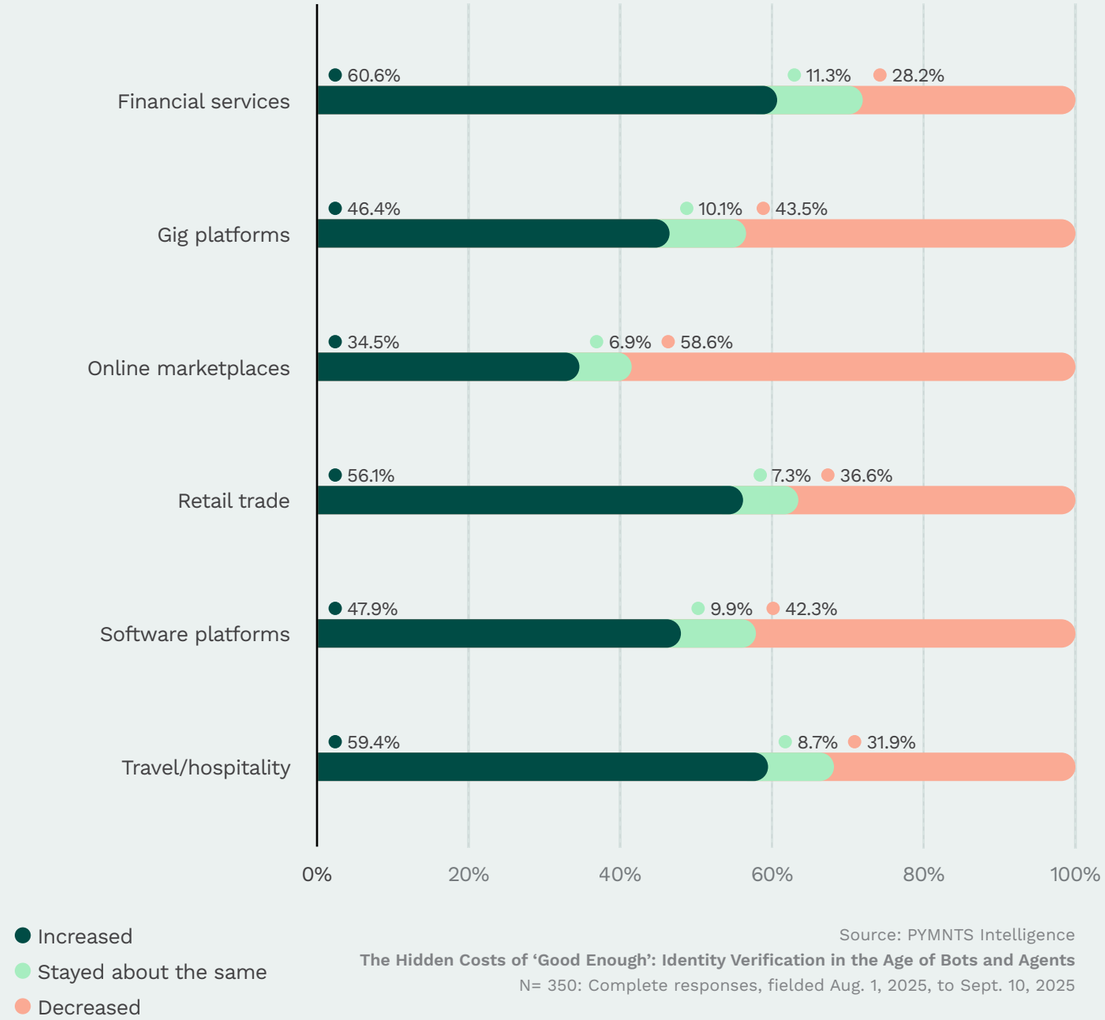


Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Not every company reports a growing menace from adversarial bots. Nearly four in 10 (38.3%) firms say their bot traffic decreased over the last 12 months, likely because they use global digital identity systems. Twenty-eight percent of financial services firms saw a 28% drop, as did 32% of travel and hospitality firms, 37% of retail trade companies, 42% of software platforms, 44% of gig platforms and 59% of online marketplaces.

FIGURE 10:

How specific industries have experienced bot traffic over the past 12 months



Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

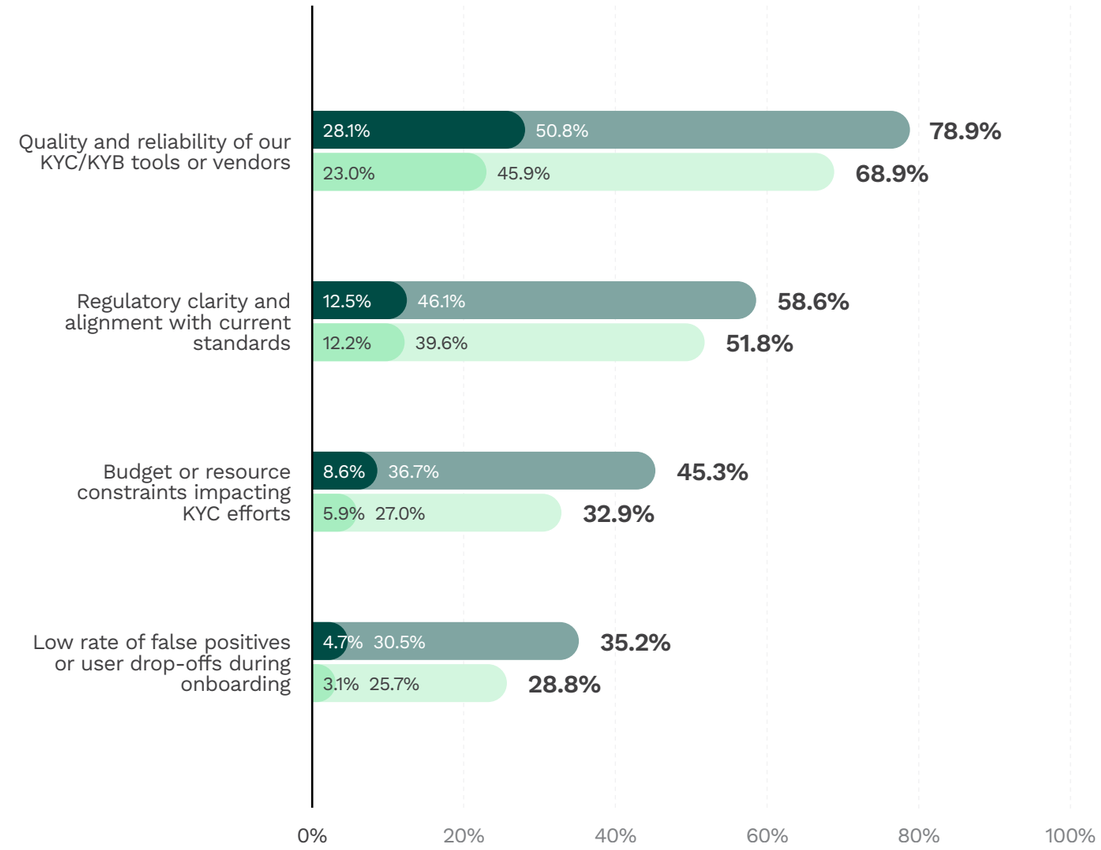
Global platforms boost identity accuracy, speed and trust.

An identity platform that is global in its capabilities has major advantages over one that is narrowly focused on a geography or niche. It uses international data sources to authenticate the identities of individuals and businesses across different countries, comply with KYC and AML requirements across jurisdictions and provide secure, streamlined onboarding for consumers and customers around the world.

Companies with a global reach need far more than a platform geared only to the country where they’re headquartered. Nearly eight in 10 companies, or 78.9%, that use a global identity platform cite the quality and reliability of their chosen vendor as giving them confidence in authenticating the identities of the far-flung consumers, business customers and suppliers they deal with. Global platforms deliver more than verification for companies operating in multiple markets; they also serve as a lever for growth.

FIGURE 11:

Factors that are either frequent or the most common for confidence in identity verification



Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Firms using global platforms report greater confidence in their verification quality, clarity and efficiency, and achieve lower declines and false positives. Nearly two in three (65.6%) companies using global platforms report lower digital transaction decline rates year-over-year compared to companies deploying an identity system without a globally integrated reach. Nearly as many, or 62.5%, also see false positives decline. Fewer false declines means fewer lost sales and fewer frustrated customers. By cutting both declines and false positives, global identity platforms protect revenue while improving customer trust, a dual advantage that fragmented solutions can’t match.

63%

of companies using globally integrated platforms **report lower false positive rates** compared to the prior 12 months.

FIGURE 12:

Decrease in decline rate for digital transactions

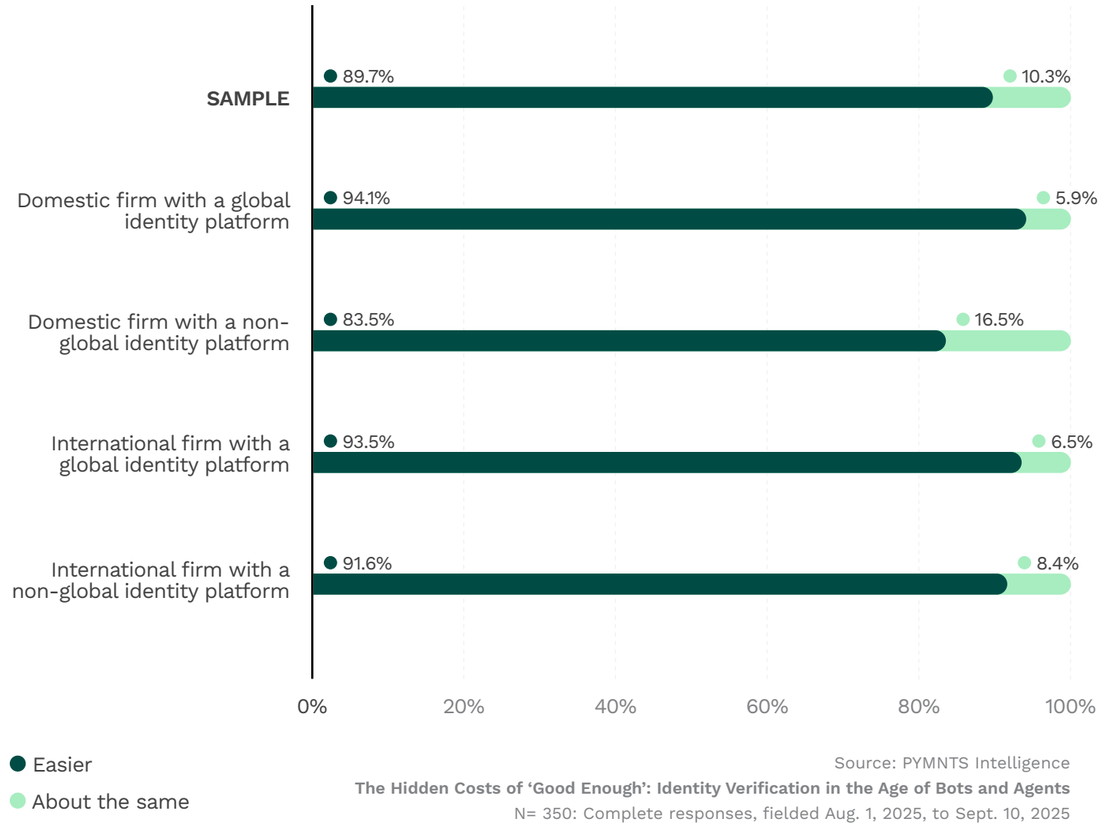
Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

A global identity platform is essential to reducing operational drag and making authentication management easier.

More than eight in 10 companies (83.4%) using global identity platforms rate their system as high performing. Nearly 94% say global identity platforms make it easier to manage their compliance and AML regulations. By contrast, firms relying on non-global identity solutions face higher operational drag. Only 83.5% of those users say it’s easier to manage identity verification. In short, an integrated identity platform isn’t just about reducing declines and false positives; it’s also about lowering operational burdens and future-proofing compliance.

FIGURE 13:

Change in difficulty meeting KYC/KYB requirements over time

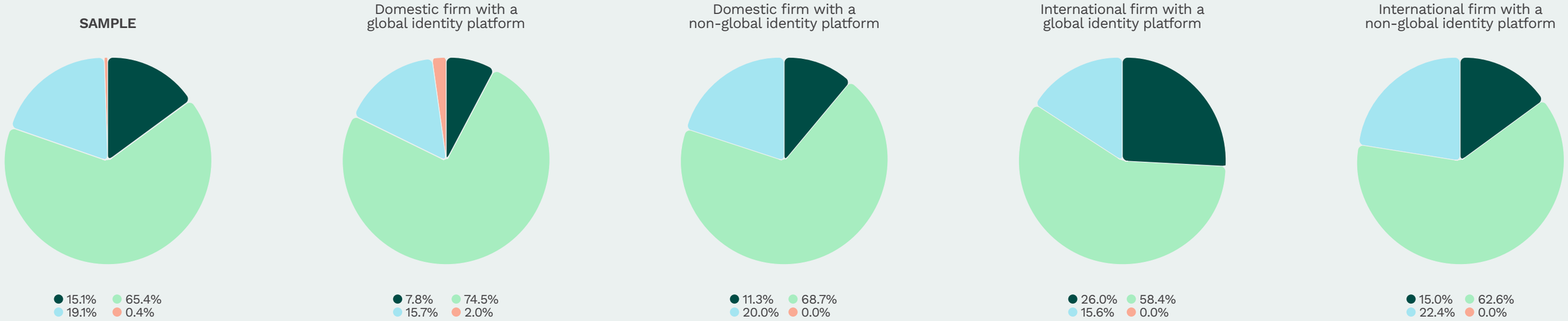


Source: PYMNTS Intelligence
The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

Among international firms with a global customer and supplier base, 84.4% that use an integrated global identity system say their technology either “performs well” or is “best-in-class.” In contrast, just 77.6% of international companies not using such a system say the same. Unlike stand-alone data checks or manual oversight, global identity platforms consistently deliver fewer issues, stronger performance and a clear strategic advantage. The data make it clear that global platforms deliver higher confidence and stronger performance across the board and are better equipped to handle cross-border complexity and compliance.

FIGURE 14:

How companies rate their digital KYB/KYC systems



Source: PYMNTS Intelligence

The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents

N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

ACTIONABLE INSIGHTS

01

Recognize that you don’t truly grasp how much adversarial bots and agents are harming your business. The cost of digital identity systems that are merely “good enough” is a steep 3.1% of annual revenue. In today’s global digital economy, where consumers, business customers and suppliers are spread out over the world, businesses should reframe their investment in identity verification as a strategic initiative to protect and grow revenue, not just as a cost and compliance center.

02

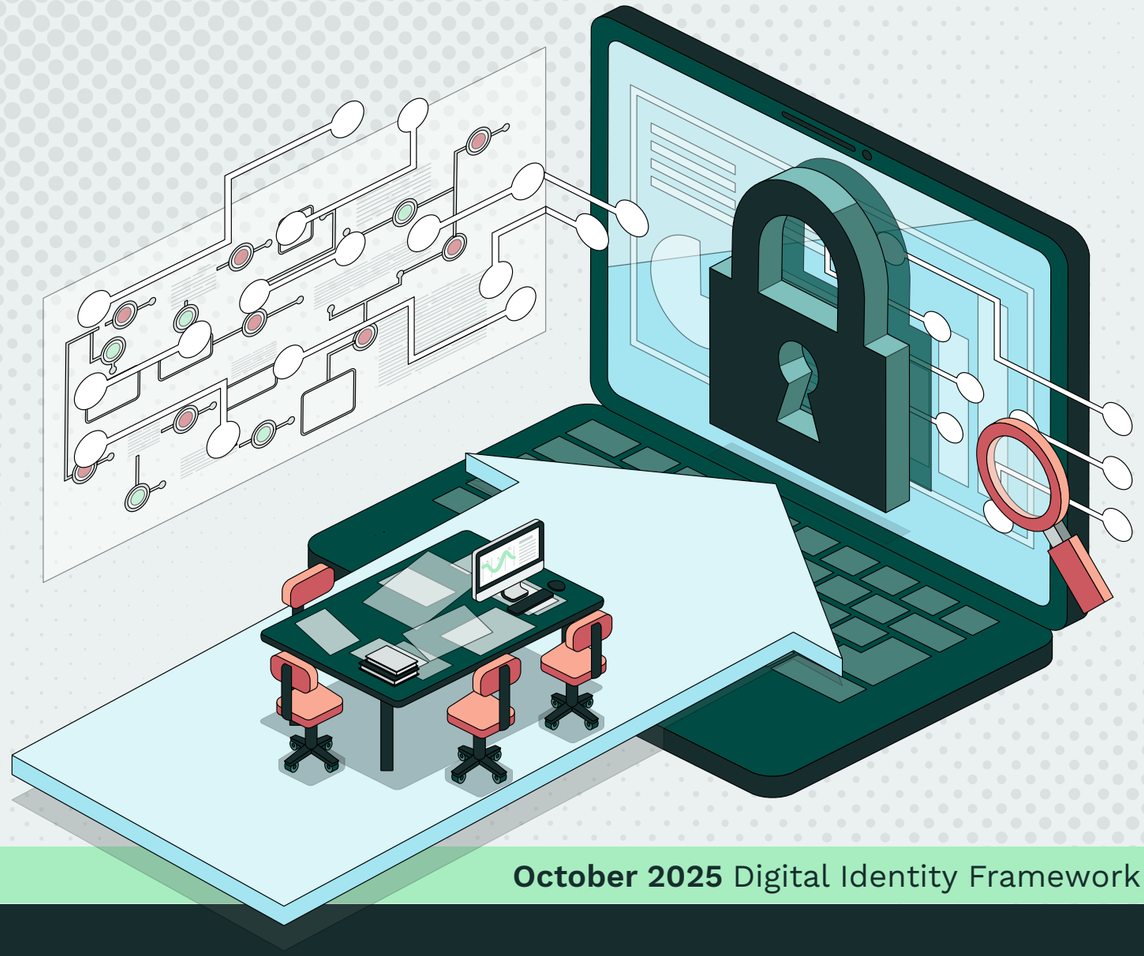
Invest in a digital identity system that can reliably distinguish between malicious bots or agents that fuel fraud and friction and helpful ones that grow business. The dangerous gap between how companies perceive their bot defenses (96% are confident) and the reality of the threat (59% struggle with bot-driven fraud) signals a need to invest in solutions that can accurately differentiate between the two.

03

Adopt an integrated global identity platform to reduce operational burdens, create a smoother customer journey and grow revenues. Fragmented identity verification systems create significant hidden costs, with half of all companies reporting poor customer experience and higher expenses from manual reviews. Use a global identity system to cut hidden operational costs and improve customer experience.

04

Deploy a global identity platform to enable international expansion. Companies relying on non-global platforms are less confident in their ability to handle cross-border complexity and compliance. Adopt a global platform to fuel greater confidence in verification quality, achieve lower false positive rates and better manage the complexities of international operations.



October 2025 Digital Identity Framework

The Hidden Costs of ‘Good Enough’

Identity Verification in the Age of Bots and Agents

PYMNTS INTELLIGENCE | Trulioo

Methodology

“**The Hidden Costs of ‘Good Enough’: Identity Verification in the Age of Bots and Agents**” is based on a survey of 350 companies conducted from Aug. 1, 2025, to Sept. 10, 2025. The report explores the effectiveness of digital identity systems in preventing fraud and driving growth. Industries surveyed included financial services, gig platforms, online marketplaces, retail trade, software platforms and travel and hospitality. Companies operate in the United States, Canada, U.K., European Union and other European countries, China, India, Japan and other Asia-Pacific countries, the Middle East, Australia/New Zealand, Africa, and Mexico and other Latin American countries.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT:

Lynnley Browning
Managing Editor

Franco Coraggio
Analyst

Matthew V. Albrecht
Senior Research 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.