January 2026

Digital Identity Framework

When 'Good Enough' Isn't Enough

Digital Identity Verification in the Age of Bots and Agents

PYMNTS INTELLIGENCE | Trulioo

When ‘Good Enough’ Isn’t Enough

Table of Contents

PYMNTS INTELLIGENCE | Trulioo

When ‘Good Enough’ Isn’t Enough: Digital 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.

Executive **Summary**

Financial Services institutions operate in an increasingly digital environment, where identity verification now underpins both revenue generation and risk management. With 76% of financial services firms earning at least three quarters of their revenue through digital channels, any friction or inconsistency in know-your customer and know-your business (KYC/KYB) processes carries amplified business and operational consequences.

Financial services firms report some of the highest levels of identity-related friction among all industry verticals. Nearly 75% say that identity verification technologies produce inconsistent results. More than half report excessive checks that frustrate customers and slow onboarding, while many cite differing outcomes across identity platforms. These issues contribute to operational strain, higher manual review costs and points of failure in digital engagement.

Identity challenges also translate directly into financial and strategic losses. Just over three in four institutions say identity processes prevent them from expanding customers, markets or geographies, while revenue losses from KYC/KYB failures average 3%, totaling nearly $34 billion industrywide. Synthetic identity fraud, regulatory violations and account takeover represent the costliest threats.

Despite these pressures, financial services firms express strong confidence in their systems: 84% rate their KYC/KYB processes as performing adequately or better, and nearly 23% consider them best in class. This confidence is rooted in reliance on dependable vendors, familiar workflows and routine oversight, factors that reinforce a perception that current systems are “good enough.” Yet global identity platform users report easier KYC/KYB experiences, suggesting that firms may be missing measurable improvements available through more advanced solutions.

Key Findings

This research explores how identity weaknesses in financial services drive friction, block expansion and increase both fraud and regulatory exposure. As financial services firms become more digitally dependent, the limitations of “good enough” identity systems become more costly, underscoring the shift toward integrated, high-reliability verification platforms

01

Digital dependence amplifies identity risk and friction in financial services:

The industry's digital-first model heightens the cost of identity threats and the friction caused by inconsistent verification results.

02

Identity breakdowns create both missed opportunities and measurable losses:

76.1% of financial services companies report missing growth opportunities due to KYC/KYB processes, while direct revenue losses from identity failures total nearly $34 billion.

03

‘Good enough’ identity systems keep financial services firms confident, but not competitive:

Despite strong reliance on trusted vendors and familiar workflows, financial services companies face persistent friction, missed opportunities and greater losses, suggesting their confidence may not reflect true performance.

#1

Digital dependence amplifies identity risk and friction in financial services.

The industry's digital-first model heightens the cost of identity threats and the friction caused by inconsistent verification results.

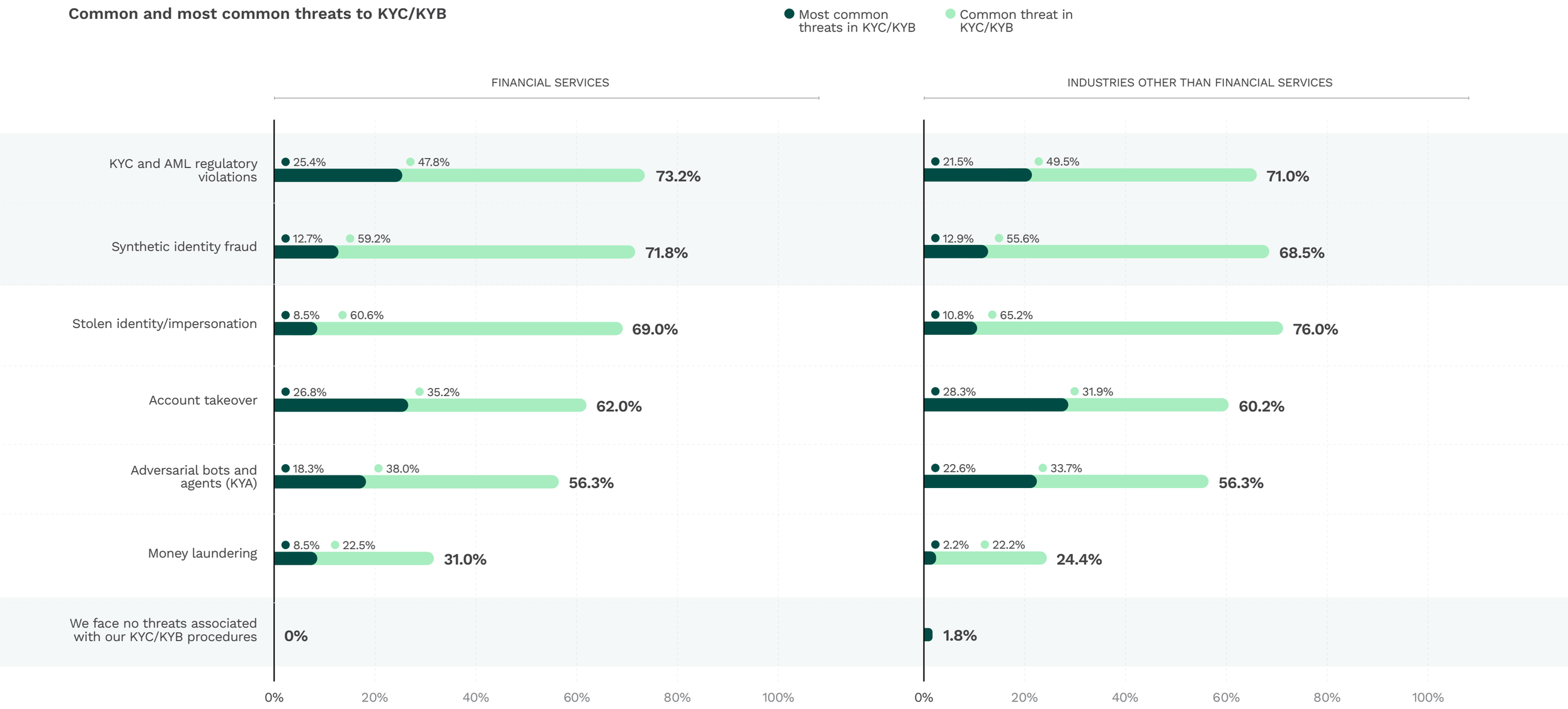
76%

of financial services firms report making at least three-quarters of their revenue from digital channels.

The financial services industry relies heavily on digital revenue streams; 76% of firms make at least three-quarters of their revenue through digital channels. This dependence on digital engagement amplifies the impact of KYC and KYB challenges, which firms report at some of the highest rates in the sample. Synthetic identity fraud, account takeover, money laundering and regulatory violations all appear more frequently for the sector than for many other verticals, creating both financial and operational risk in the very channels where they generate most of their revenue.

FIGURE 1:

Common and most common threats to KYC/KYB



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

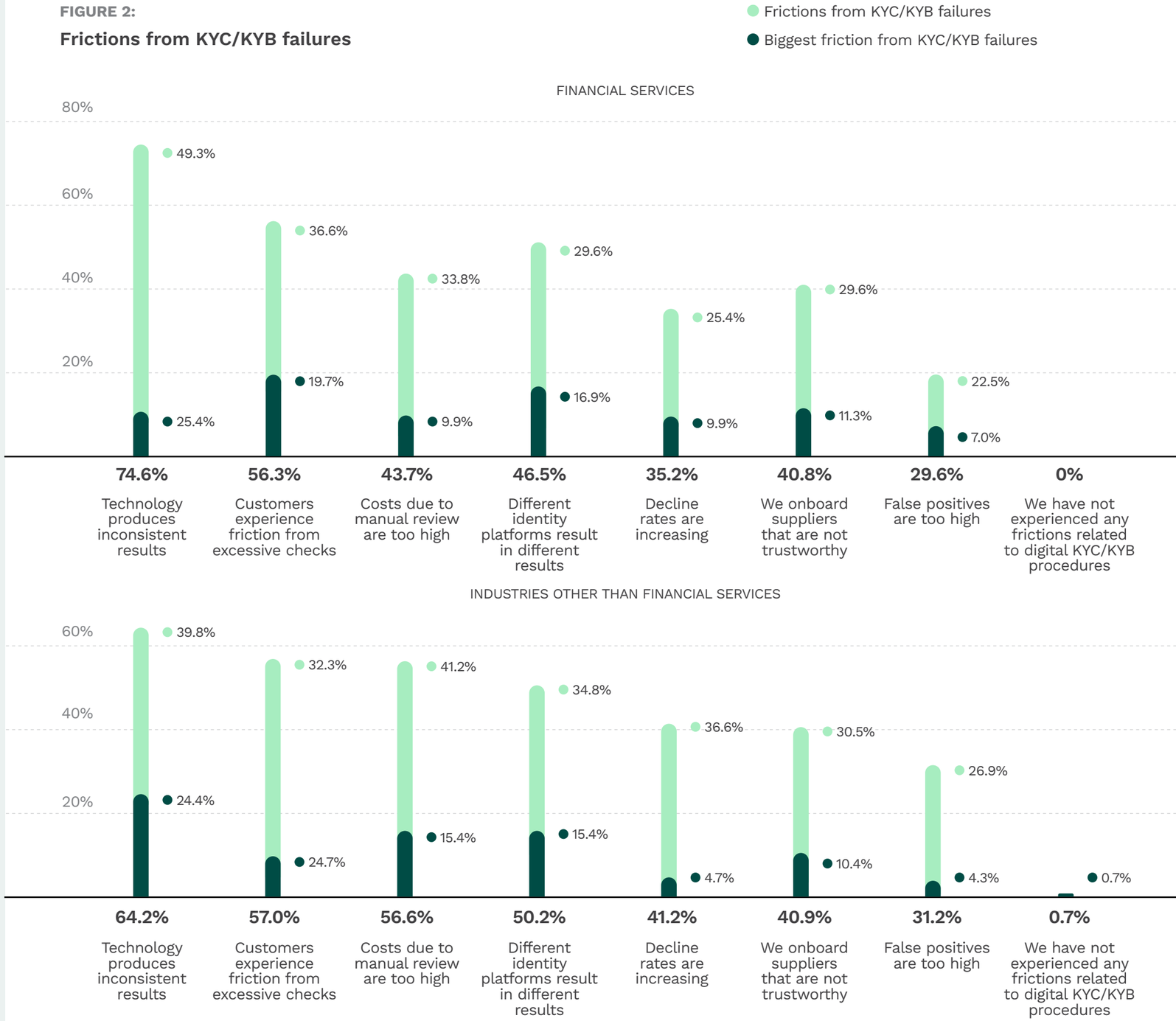
74.6%

of financial services firms say verification technology produces inconsistent identity results.

Financial services firms report high levels of friction linked to KYC and KYB processes, with inconsistent technology results cited by about 75% of respondents. Excessive checks that create customer friction affect roughly 56%, while 44% say manual review costs are too high. Nearly half of firms report differing results across identity platforms, contributing to operational inconsistency. Additional issues include rising decline rates and difficulty verifying suppliers, both affecting around 35% of firms. Every firm reported experiencing some friction, underscoring the widespread operational strain created by identity workflows.

FIGURE 2:

Frictions from KYC/KYB failures



Source: PYMNTS Intelligence

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

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

#2

Identity breakdowns create both missed opportunities and measurable losses

76.1% of financial services firms report missing growth opportunities due to KYC/KYB processes, while direct revenue losses from identity failures total nearly $34 billion.

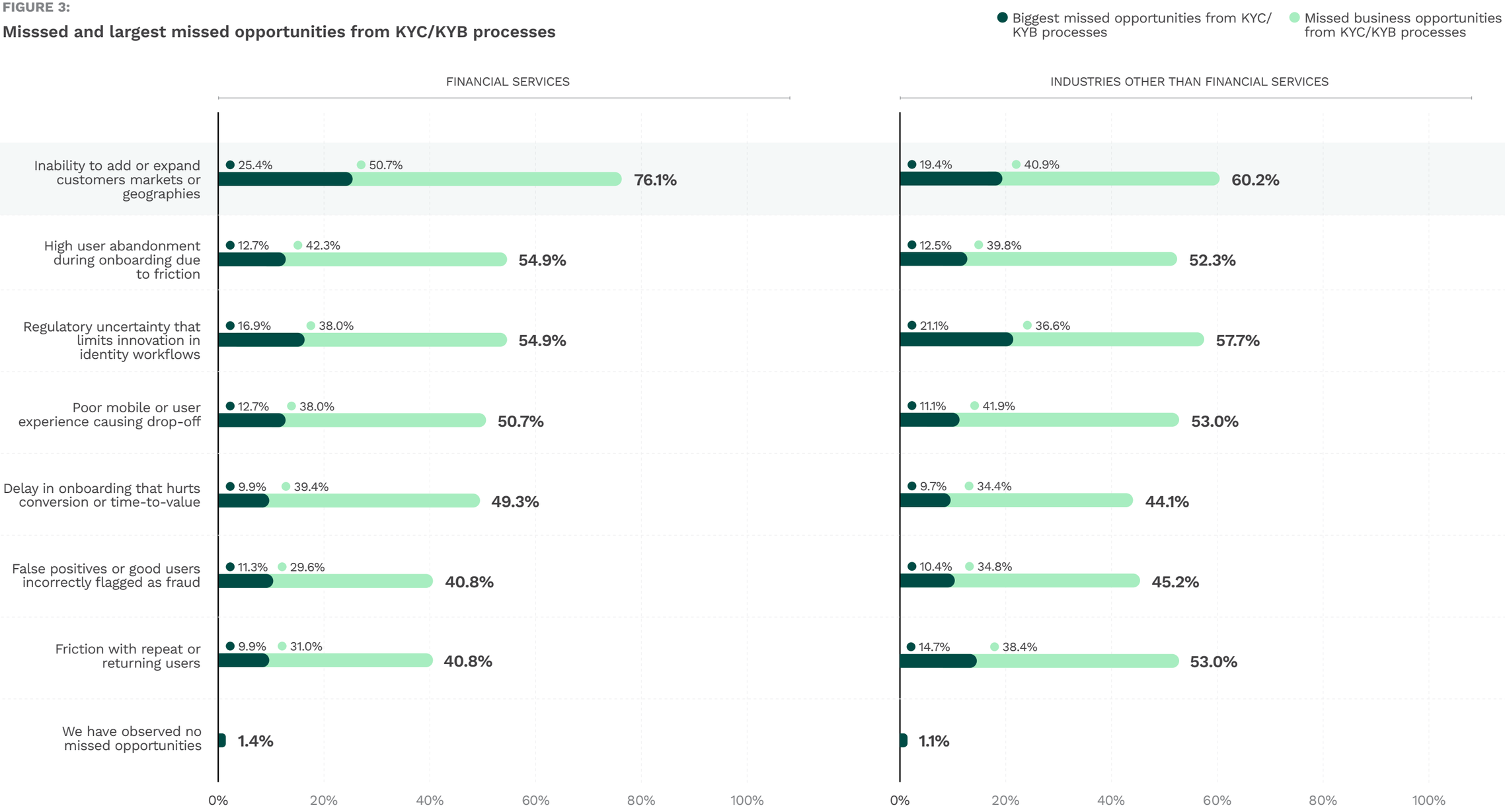
76.1%

of financial services firms say identity processes prevent them from expanding customers, markets or geographies.

Financial services firms cite significant missed business opportunities tied to their current KYC and KYB processes. The most common impact is an inability to add or expand customers, markets or geographies (76%), indicating that identity requirements are restricting growth at the top of the funnel. High user abandonment during onboarding remains a major drag on conversion, with 55% citing friction related drop off. Regulatory uncertainty also limits innovation for 55% of firms, while 51% report poor user experience as a source of lost business. Delays in onboarding (49%) and false positives that misclassify legitimate users as fraudulent (41%) further compound these challenges, illustrating how both compliance and experience issues converge to suppress growth.

FIGURE 3:

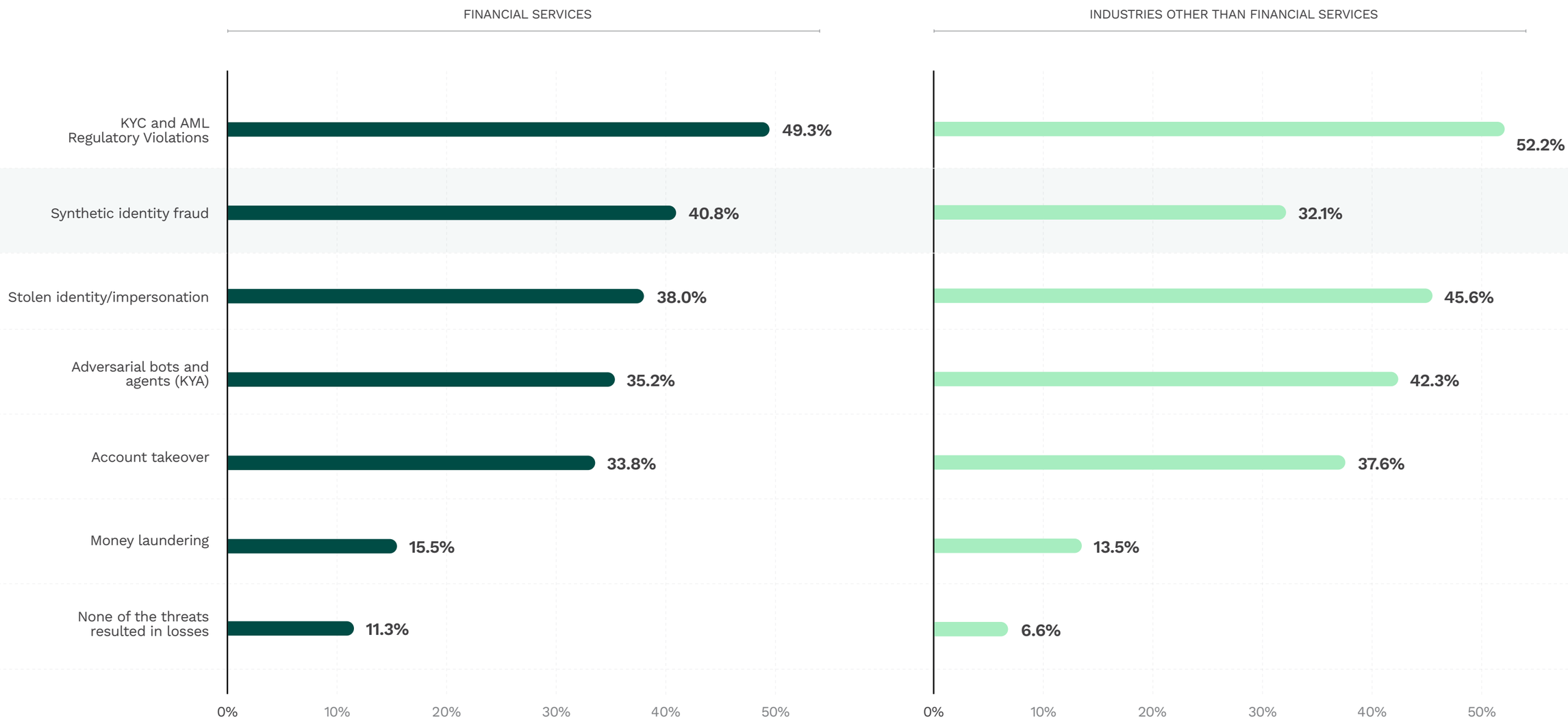
Misssed and largest missed opportunities from KYC/KYB processes



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

FIGURE 4:

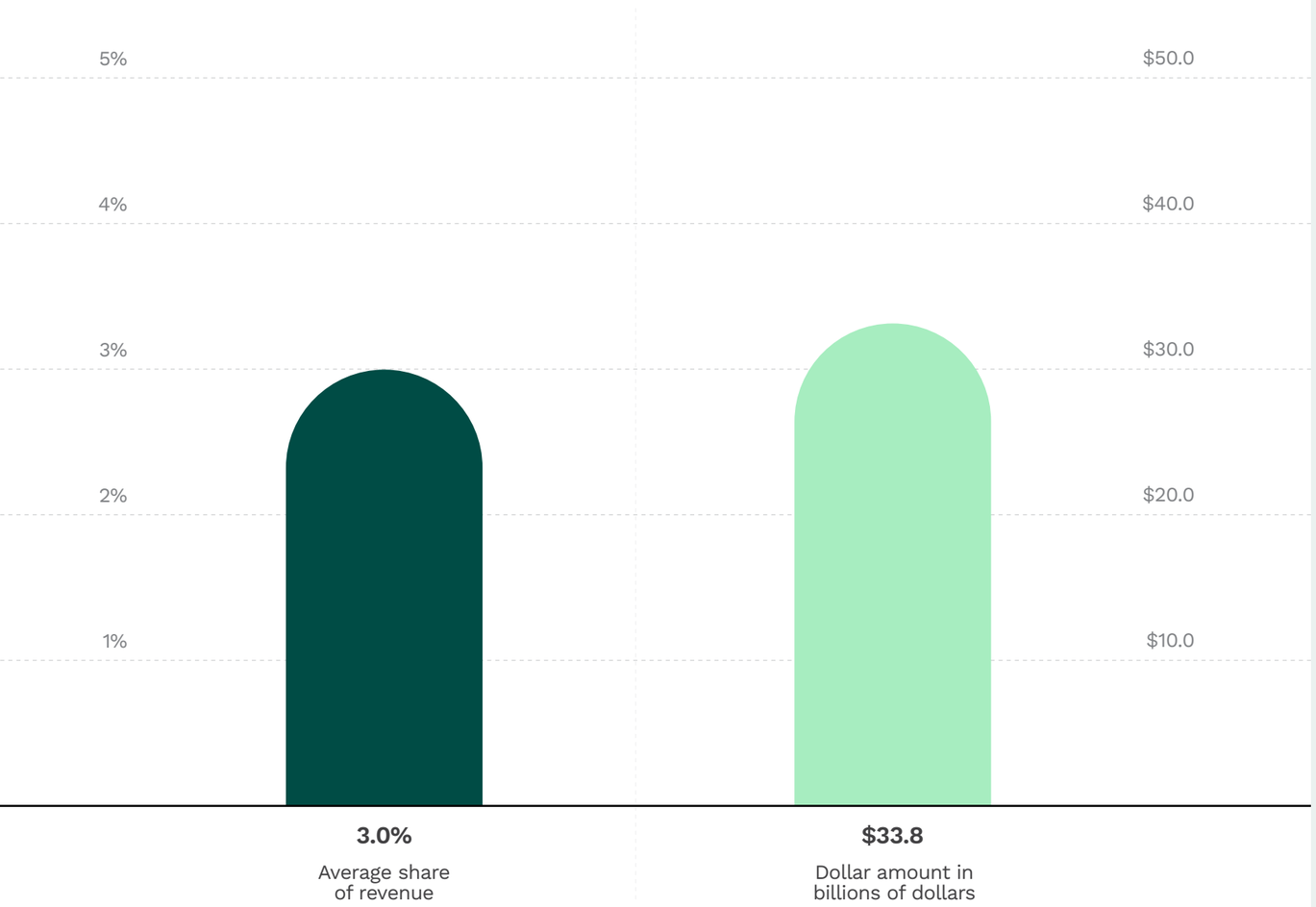
Reported incidents or losses due to identity verification failures



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

FIGURE 5:

Revenue loss due to failure in KYC/KYB procedures, by industry



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

3%

Reported revenue loss among financial service firms stemming from KYC/KYB failures, resulting in nearly $34 billion a year across the industry.

Financial services firms report meaningful losses across multiple identity related threats, with synthetic identity fraud (40.8%) emerging as one of the costliest. Synthetic fraud involves criminals creating new fictitious identities using a mix of real and fabricated information, such as pairing a stolen Social Security number with a fake name or address. These constructed profiles often pass traditional verification checks, enabling fraudsters to build credit, open accounts and take out loans that are never repaid. Losses tied to KYC/AML violations (49%), stolen identity/impersonation (38%) and account takeover (33.8%) are also widespread, underscoring how gaps in verification directly translate into financial and compliance risk. Only 11% of financial services firms avoided losses entirely, highlighting how pervasive these challenges remain.

#3

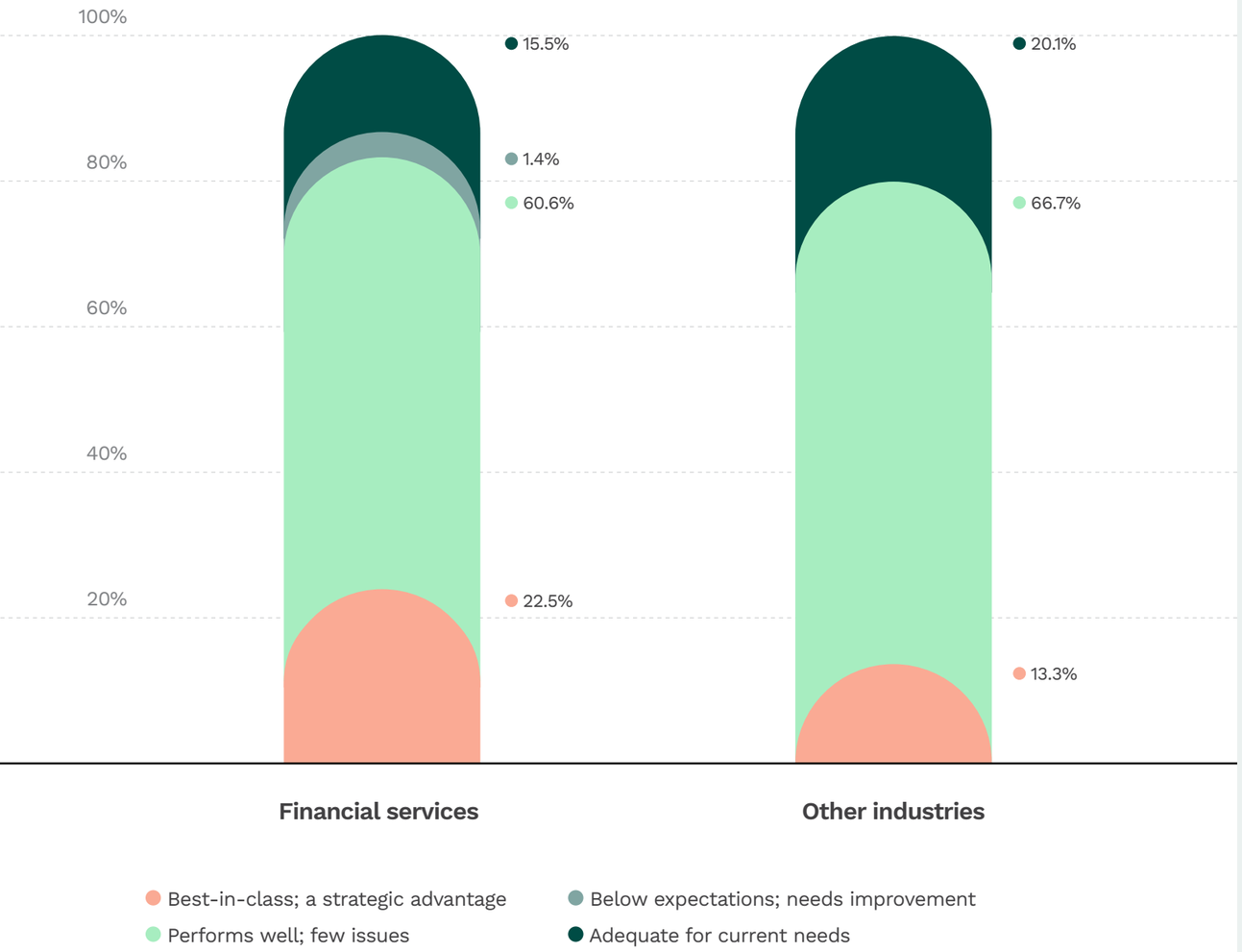
‘Good enough’ identity systems keep financial services firms confident, but not competitive:

Despite strong reliance on trusted vendors and familiar workflows, firms face persistent friction, missed opportunities and greater losses, suggesting confidence may not reflect true performance.

Financial services firms maintain strong confidence in their KYC and KYB systems, even as they report high friction, greater missed opportunities and more revenue loss than other industries. Nearly 23% rate their systems as best in class, and another 61% say they perform well with few issues. This elevated self assessment suggests that incremental improvements and familiarity with existing workflows reinforce a sense that current systems are “good enough,” despite evidence that identity-related challenges continue to impact growth and resilience.

FIGURE 6:

Overall rating of digital KYC/KYB systems



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

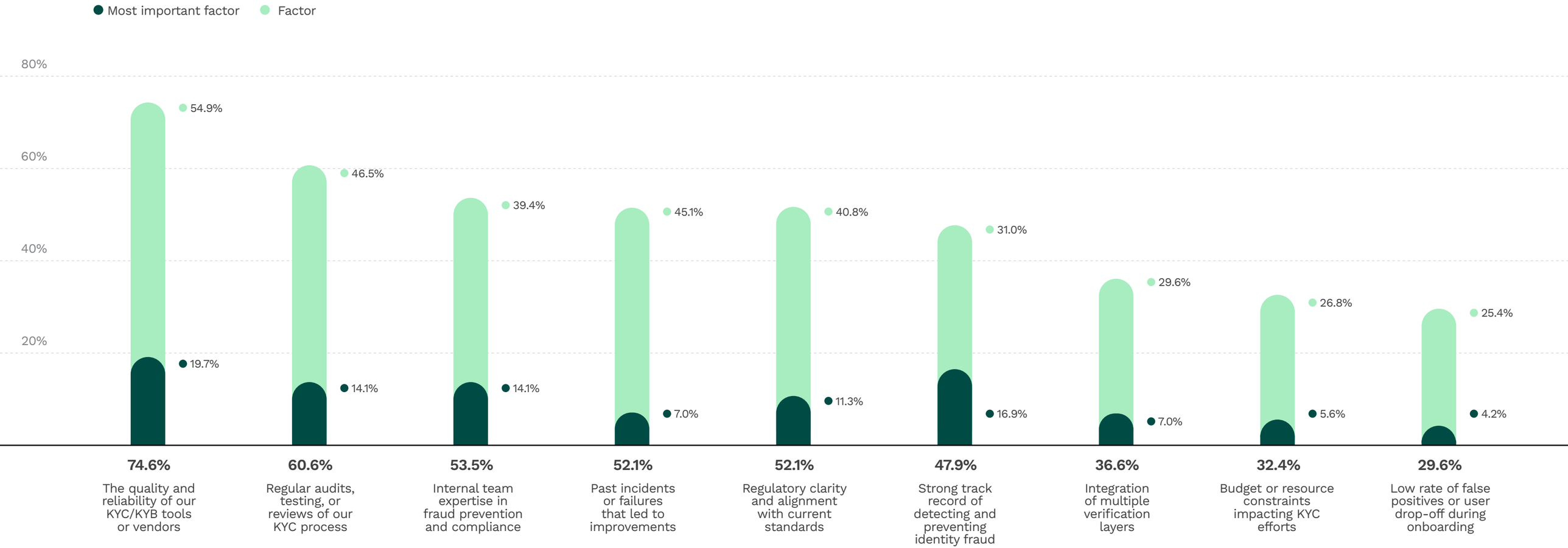
92.3%

of financial services firms using a global ID platform report less difficulty in KYC/KYB over time.

Financial services firms’ belief that their identify verification systems are performing well stems from their reliance in familiar workflows and regular oversight, reinforcing a sense that things are "good enough." Yet earlier findings show that friction, missed opportunities and revenue loss persist, suggesting that their confidence may overstate how effectively these systems are truly performing. In contrast, 92.3% of all global identity platform users report that KYC/KYB has become easier over time, underscoring how more advanced solutions deliver measurable improvements that financial services firms may be missing out on.

FIGURE 7:

Factors Behind Confidence in Identity Verification & Most Important Factor Behind Confidence in Identity Verification



Source: PYMNTS Intelligence
When ‘Good Enough’ Isn’t Enough: Digital Identity Verification in the Age of Bots and Agents
N= 350: Complete responses, fielded Aug. 1, 2025, to Sept. 10, 2025

January 2026

Digital Identity Framework

When ‘Good Enough’ Isn’t Enough

Digital Identity Verification in the Age of Bots and Agents

PYMNTS INTELLIGENCE | Trulioo

Methodology

When ‘Good Enough’ Isn’t Enough: Digital 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., the EU and 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

Matthew V. Albrecht
Senior Research Analyst

Franco Coraggio
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.

DISCLAIMER

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