March 2026

Digital Identity Framework

Identity at Scale:

Where KYC/KYB Touchpoints Create (or Contain) Agent Risk

PYMNTS INTELLIGENCE | Trulioo

Identity at Scale

READ MORE

January 2026

Report Title:

When 'Good Enough' isn't Enough

PYMNTS INTELLIGENCE | Trulioo

Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk 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**

Digital identity verification has evolved into a process that goes far beyond confirming who a new customer is at onboarding. It now spans multiple customer workflows, including login/access, transactions, fraud monitoring and lending.

Firms report using digital verification checks in 4.4 workflows on average, with usage highest for frequent activities like login/access and online transactions. As identity controls expand across workflows, identity risk becomes interconnected. Customer and business verification increasingly occur within the same operational flows, meaning that misclassification of a customer or enforcement gaps can propagate through counterparties and downstream systems.

This playbook maps where organizations apply know your customer (KYC) and know your business (KYB) controls across core workflows (account opening, login/access, transactions, onboarding, fraud monitoring, vendor onboarding, and lending). It also shows how agent-driven threats (adversarial bots and automated/agent-assisted abuse), referred to here as know your agent (KYA), surface across that entire stack.

KYA is widely reported as a threat, especially in high-stakes areas like loan applications. But the data shows clear differences in this threat based on how widely identity controls are used. Companies with identity controls in only three to four workflows report more intense KYA pressure and worse downstream outcomes in our measures, more missed opportunities, greater customer friction and more breakdowns caused by false positives (misclassifying legitimate users as fraudulent) or the onboarding of untrustworthy entities. In contrast, companies operating higher-density programs (across five or more workflows) are more likely to adopt hybrid governance models that combine internal and external teams and to report greater operational stability over time.

Together, the findings suggest that a robust digital identity verification system is an architectural and organizational capability that determines where trust resonates with customers, suppliers, partners and platforms as agent activity scales in the agentic economy.

Key Findings

01

Identity risk is embedded, shared and systemic.

Companies use digital identity in just over four workflows on average, meaning verification now spans multiple core functions and operates as a cross-workflow control system.

02

Firms that verify identity in fewer workflows feel greater agent pressure.

The costs appear in lost revenue and increased customer and supplier friction.

Key **Findings**

03

Fewer use cases lead to more breakdowns and higher costs.

In both KYC and KYB, companies with fewer identity workflows report more control failures and higher losses related to identity verification.

04

Broader workflow coverage pairs hybrid oversight with operational stability.

Firms running identity verification across five or more workflows are about twice as likely to use internal and third-party teams, and nearly all report KYC/KYB difficulty is stable or improving year over year (96% to 98%).

1

Identity risk is embedded, shared and systemic.

Firms deploy digital identity in 4.4 workflows on average, meaning verification now spans multiple core functions and operates as a cross-workflow control system.

Identity decisions are embedded across the most used workflows.

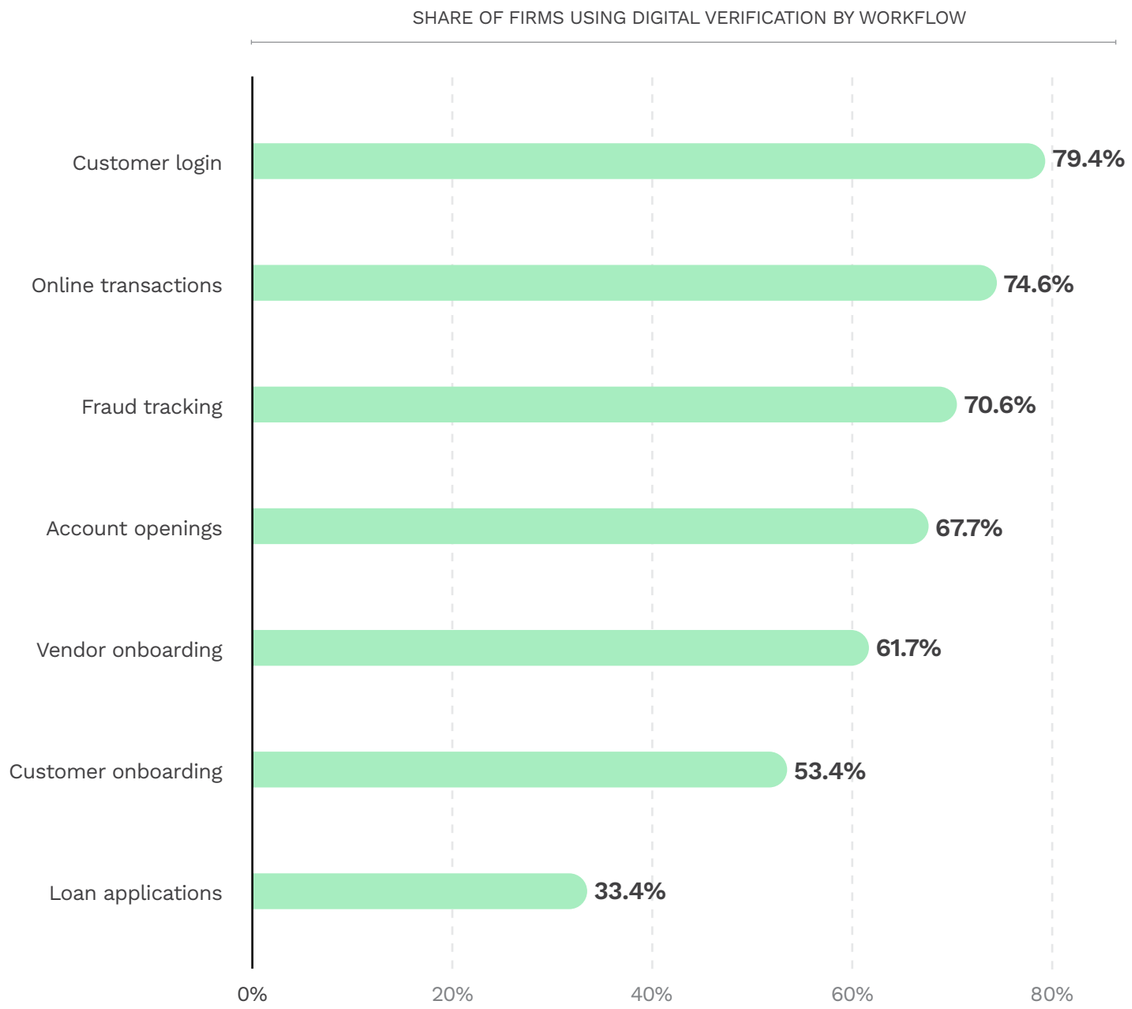
On average, companies report having 4.4 workflows for digital verification.

Digital verification isn't just about onboarding. Nearly eight in 10 firms use it for customer login (79.4%), and roughly three-quarters (74.6%) apply it to online transactions, the two of the most common decision points for verification processes. Adoption remains broad in fraud tracking (70.6%) and account opening (67.7%), showing that identity controls are being used both to prevent misuse and to manage account risk at the front door.

Importantly, verification extends into operational workflows as well. More than six in 10 firms (61.7%) use it for vendor onboarding and 53.4% for customer onboarding. That means identity risk is shared across workflows: An issue in one place can ripple into conversion rates, fraud losses and partner trust.

FIGURE 1:

Share of firms using digital verification by workflow



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

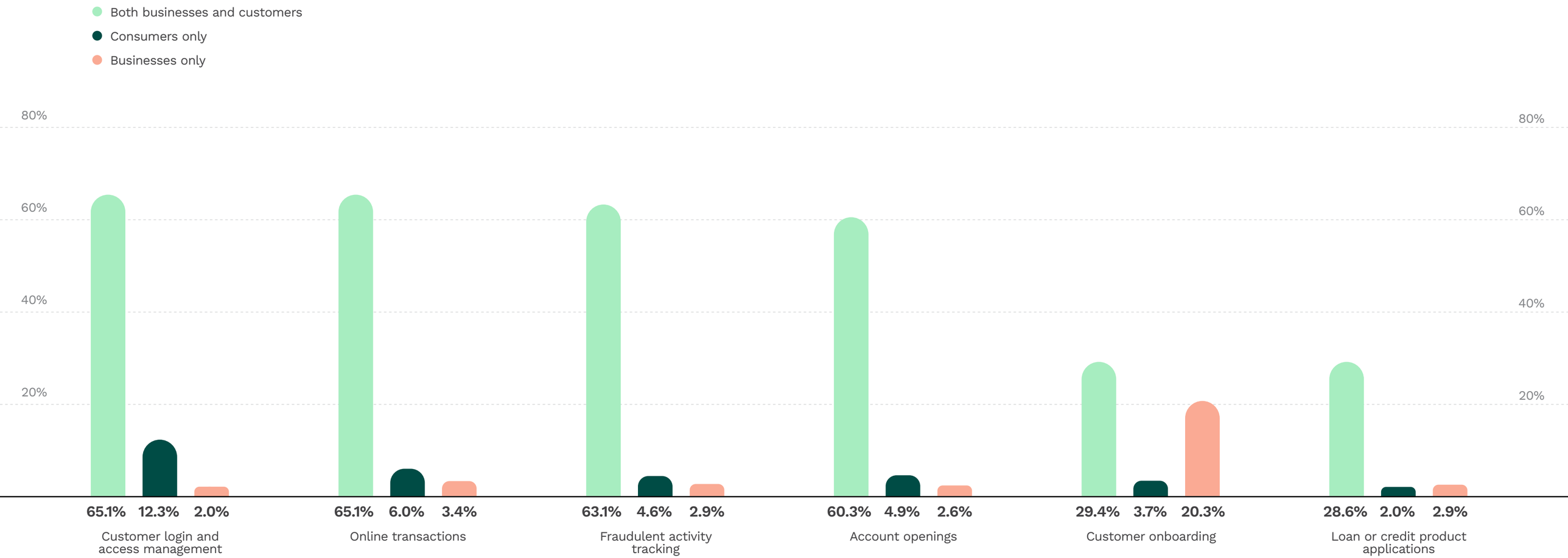
Most companies' operational identity workflows verify both businesses and customers.

Digital verification is rarely deployed in isolated KYC or KYB silos. In high-frequency workflows like login/access, transactions, fraud tracking and account opening, roughly 60% to 65% of firms verify both businesses and customers in the same flow. Verification limited to only businesses or only customers accounts for a small minority of activity.

When customer and business identity checks happen in the same workflow, errors don't stay contained. A misclassification or control failure can affect both sides of the interaction, creating false positives, friction and downstream trust issues. That's why KYA needs to sit on top of both KYC and KYB, not operate as a separate track.

FIGURE 2:

Task digitally verified or authenticated via KYC/KYB



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

Adversarial automation occurs across identity workflows, peaking in loan applications.

Nearly two-thirds (63.2%) of firms offering loan applications report KYA-type threats, the highest prevalence among identity workflows.

Adversarial bots and agents aren't confined to a single identity checkpoint—they appear consistently across all workflows where firms deploy digital verification.

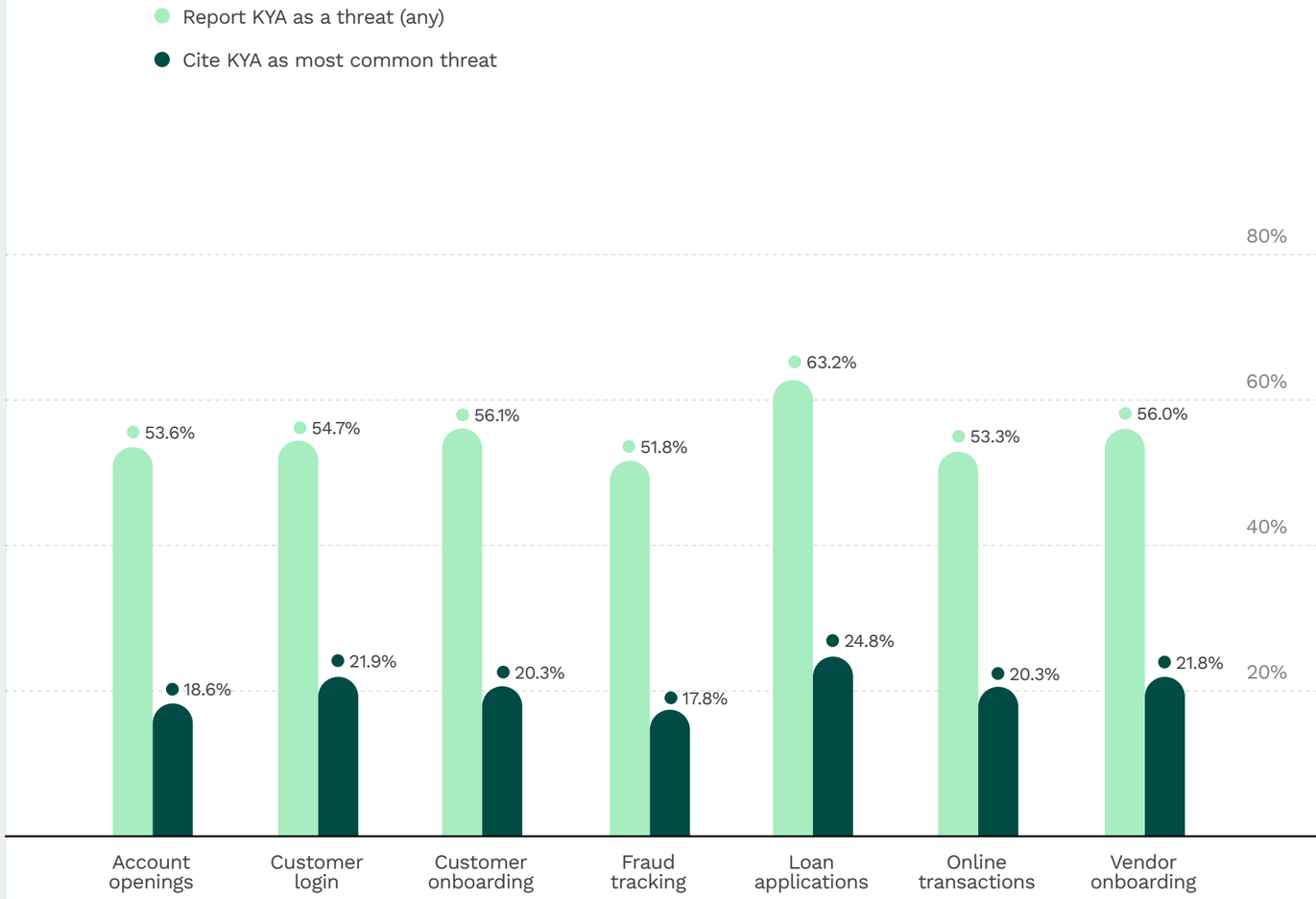
Roughly half to nearly two-thirds of firms using verification in core processes, including login, onboarding, transactions, fraud tracking and vendor onboarding, cite KYA as a threat.

Loan applications represent the most concentrated exposure point, with 63.2% reporting KYA threats and 24.8% citing it as the most common threat. This pattern suggests that automation pressure intensifies in high-value, high-stakes decision flows.

As identity verification expands throughout the operating stack, KYA becomes a cross-workflow control challenge in which misclassification, inconsistent enforcement or model blind spots in any one workflow can propagate downstream risk.

FIGURE 3:

KYA threat prevalence and intensity by workflow



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

2

Firms that verify identity in fewer workflows feel greater agent pressure.

The costs appear in lost revenue and increased customer and supplier friction.

Companies using identity checks more widely across all customer touchpoints report feeling less pressured by bots.

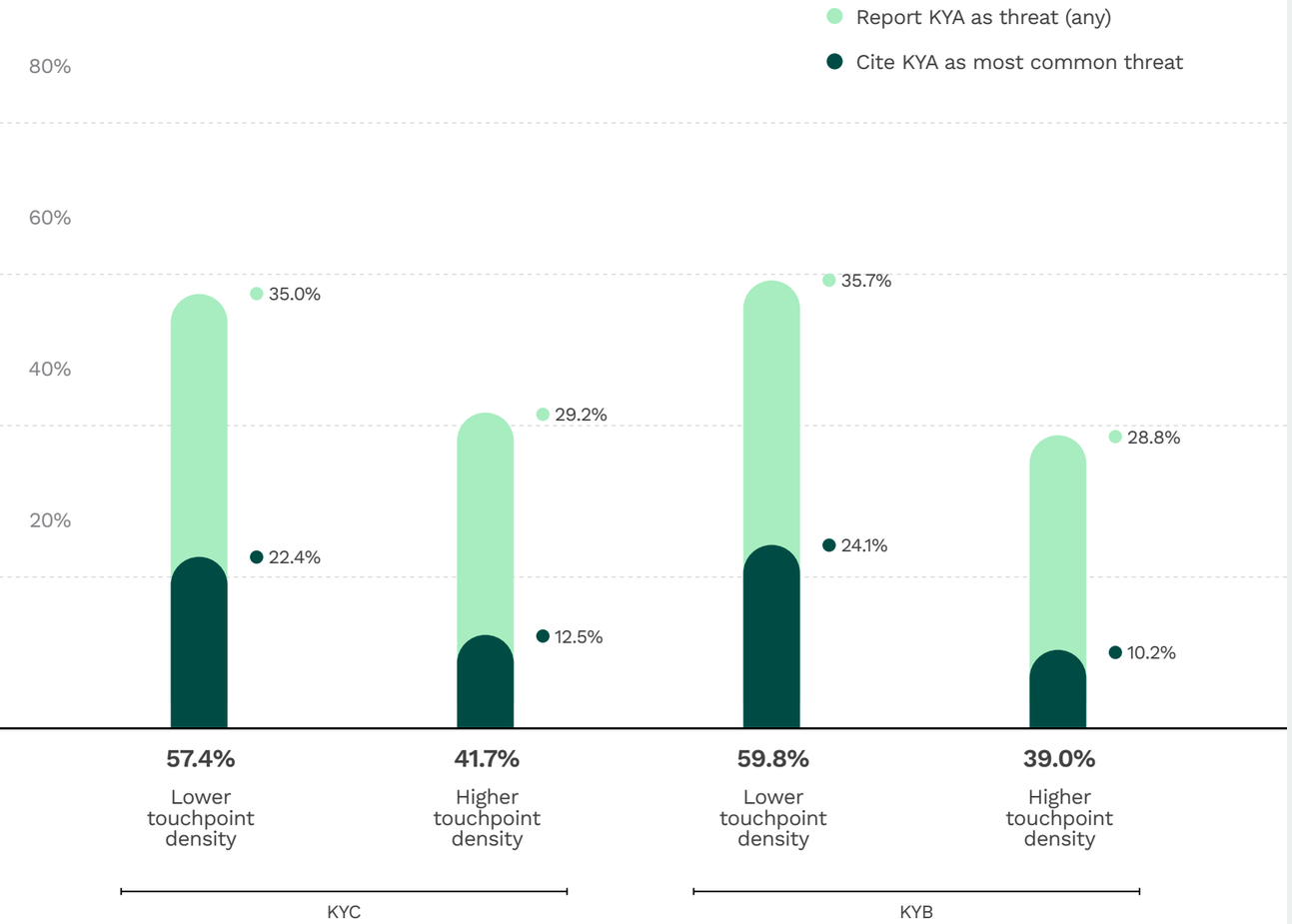
Firms that use digital identity checks in more workflows report less agent/bot pressure than firms that use them in fewer workflows. Agent/bot activity is still common in both groups, but higher-coverage firms are less likely to rank agents/bots as their single most common threat. This association is consistent with, though not proof of, stronger detection, clearer ownership and more consistent enforcement practices in more mature identity programs.

By contrast, firms with identity checks concentrated in only a few workflows may be more likely to treat bot activity, fraud losses or user friction as episodic problems rather than a cross-workflow control issue. As identity decisions spread across more operational flows, inconsistencies become more costly, pushing higher-coverage firms to manage agent/bot risk as a system-wide control that must work consistently throughout the full identity stack.

INDENTITY WORKFLOW PERSONAS	
Higher-Workflow Firms	**Lower-Workflow Firms**
Run digital identity checks in **five or more workflows**	Apply digital identity in **three to four workflows**

FIGURE 4:

KYA threat reporting by identity touchpoint density (KYC vs. KYB)



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

PYMNTS INTELLIGENCE | Trulioo

Fewer identity checks are linked to more lost revenue and greater friction for customers and suppliers.

Companies that use KYC and KYB identity checks in only three to four areas report more missed opportunities.

Companies that use identity checks in only three to four areas report more customers abandoning their applications, more repeat users facing delays and more legitimate customers being wrongly blocked.

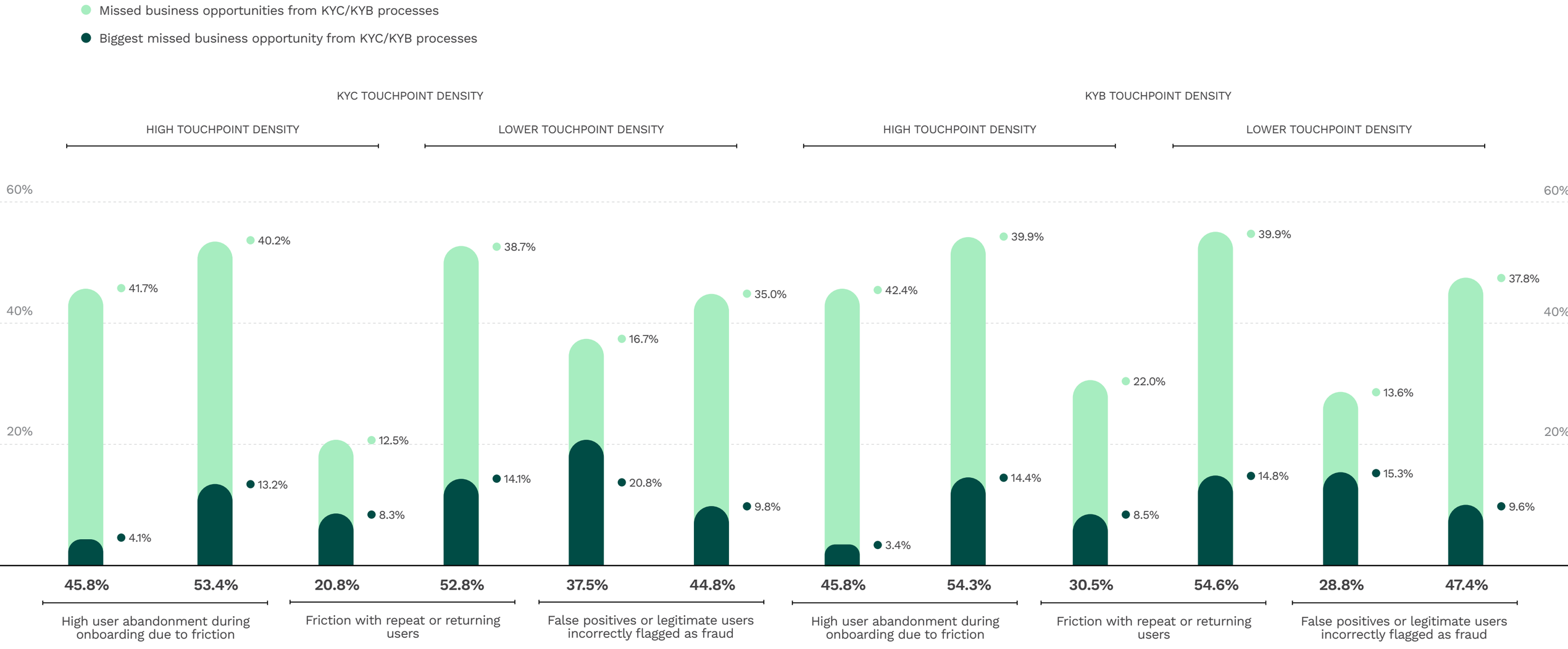
The biggest gaps appear in friction experienced by returning customers and false positives, suggesting that these firms may rely on narrower or less-tuned controls.

Conversely, companies that use identity checks more broadly appear better able to apply rules consistently, reducing unnecessary friction. That suggests they're better positioned to manage enforcement consistency across workflows.

The big picture is that as identity verification controls become embedded across the operating stack, system maturity influences not only fraud containment but also revenue retention and customer experience.

FIGURE 5:

Missed and biggest missed business opportunities from KYC/KYB processes



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

3

Using fewer identity checkpoints means more failures and higher losses.

Across KYC and KYB processes, firms using fewer digital checks report more control breakdowns and greater identity-verification-related losses.

Firms with identity checks in only three to four workflows report higher misclassification rates and greater trust gaps.

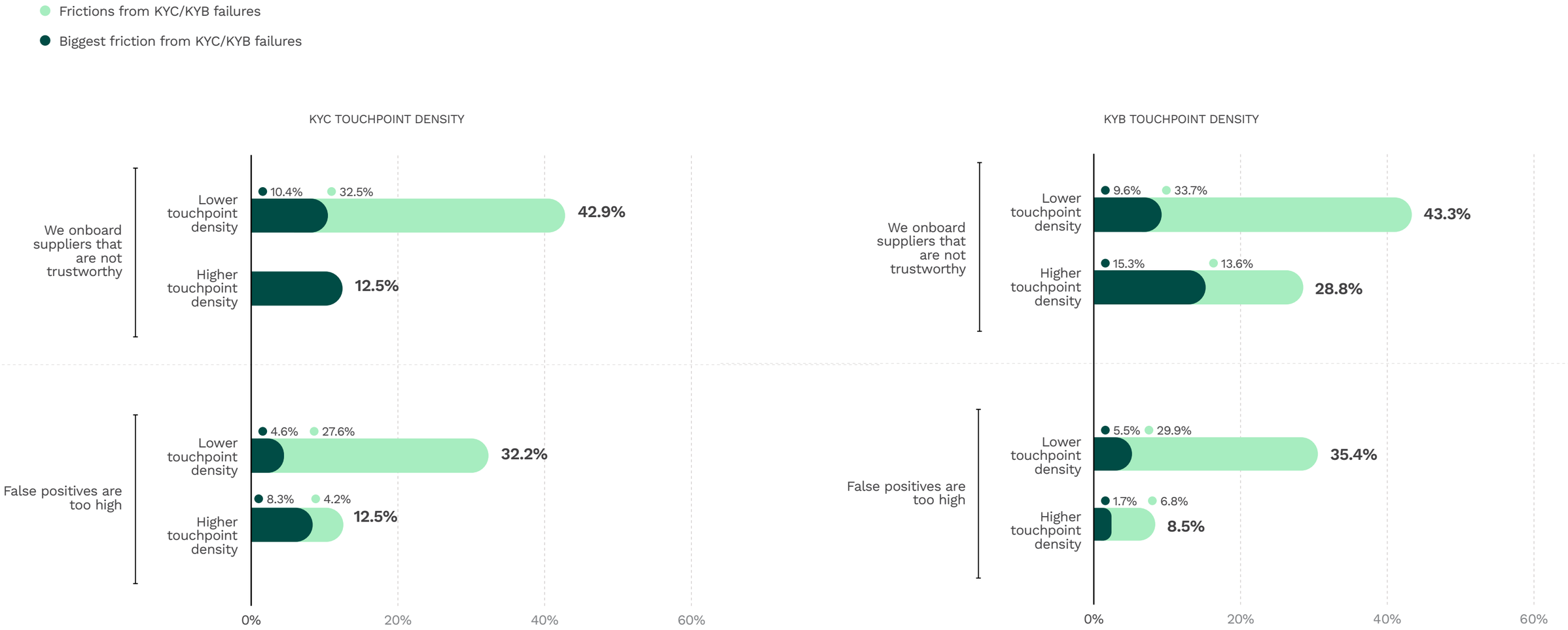
Companies using identity checks more broadly report fewer breakdowns in screening consistency.

When checks are limited to a few points, mistakes are more likely, ones that both miss bad actors and block good ones. This pattern suggests that distributed identity architectures embedded across many parts of the business, rather than handled in a single location, may enable better detection and enforcement.

Where identity controls are concentrated in fewer checkpoints, misclassification risk appears higher on both sides, blocking legitimate users while allowing problematic actors through. Identity maturity, therefore, influences not only commercial outcomes but also systemic trust and screening integrity.

FIGURE 6:

Frictions and biggest friction from KYC/KYB failures



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

Firms with fewer identity checkpoints report more KYA-related incidents or losses.

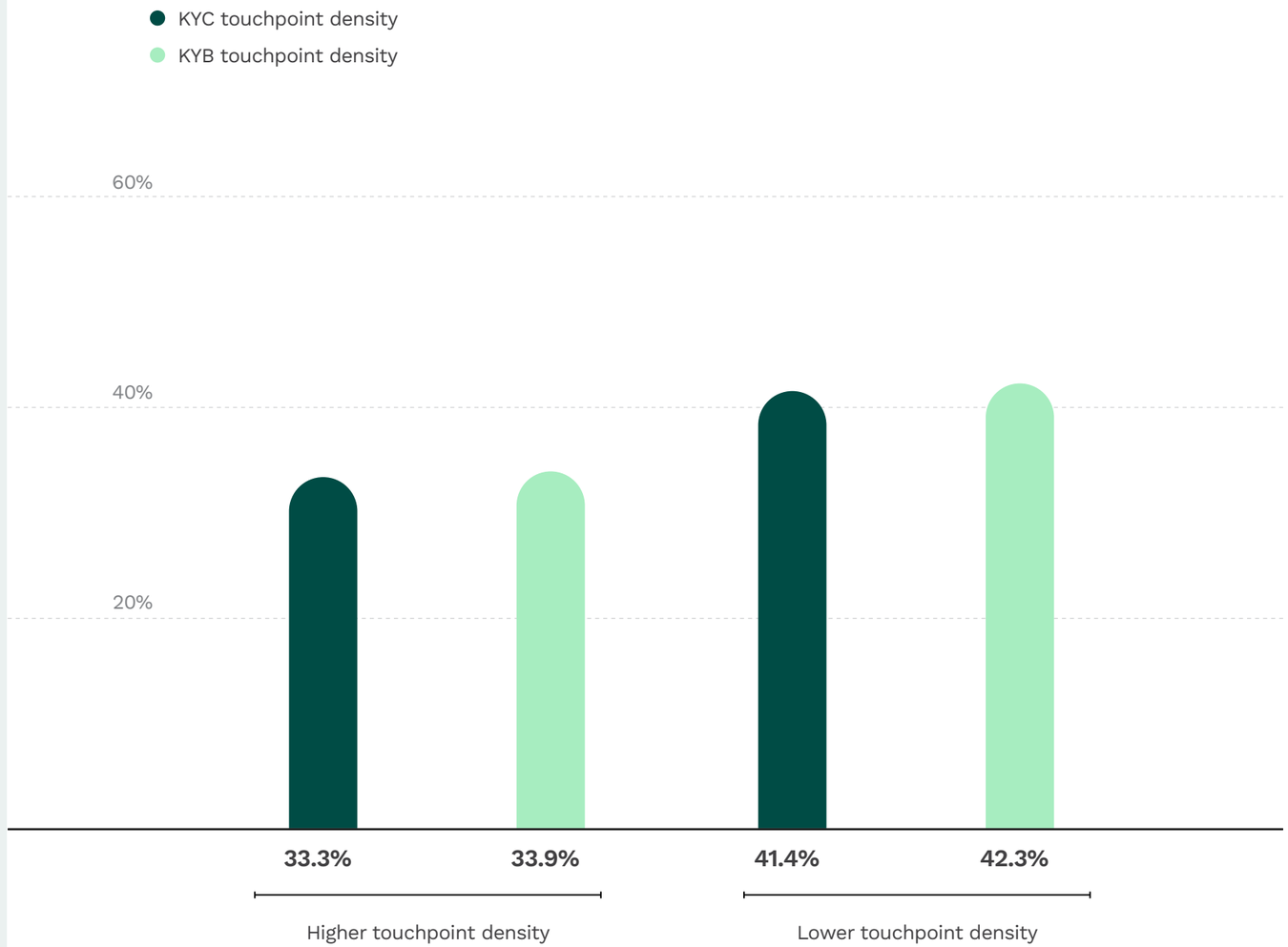
Reported incidents or losses tied to adversarial bots and agents (KYA) are widespread across identity verification workflows. Roughly four in 10 firms report incidents or losses in account openings (40.7%), customer login (39.6%), customer onboarding (41.8%) and fraud tracking (42.8%).

Exposure is materially higher in loan applications, where nearly half (48.7%) report incidents or losses, suggesting that higher-value decision points attract more automated adversarial activity. Even basic flows such as vendor onboarding (39.7%) and online transactions (35.4%) show meaningful impact.

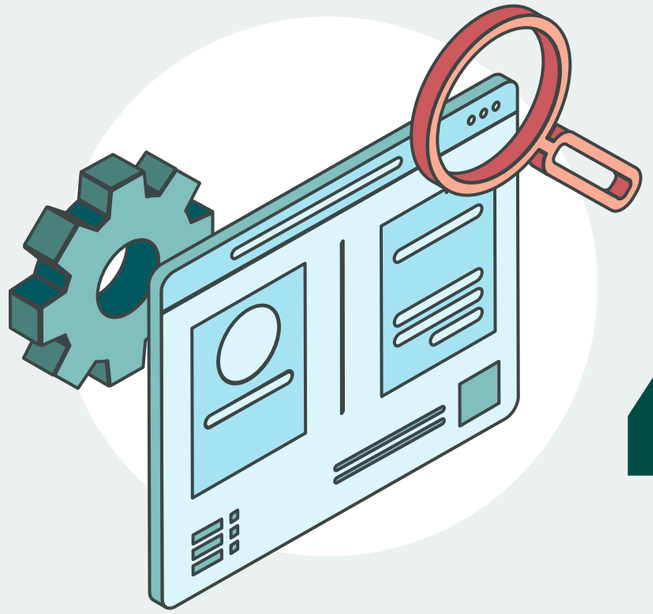
As firms expand their digital identity controls in more workflows, failures in classification, authentication or bot detection translate directly into measurable losses. High value workflows appear particularly sensitive, indicating where investment to mitigate the problem may deliver the greatest return.

FIGURE 7:

Reported incidents or losses due to identity verification failures
Adversarial bots and agents (KYA)



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025



4

Broader workflow coverage pairs hybrid oversight with operational stability.

Firms running identity verification in five or more workflows are about twice as likely to use both internal and third-party teams, and nearly all report KYC/KYB difficulty is stable or improving year over year (96% to 98%).

Companies that run identity checks in more workflows are more likely to use a hybrid (internal and external) operating model.

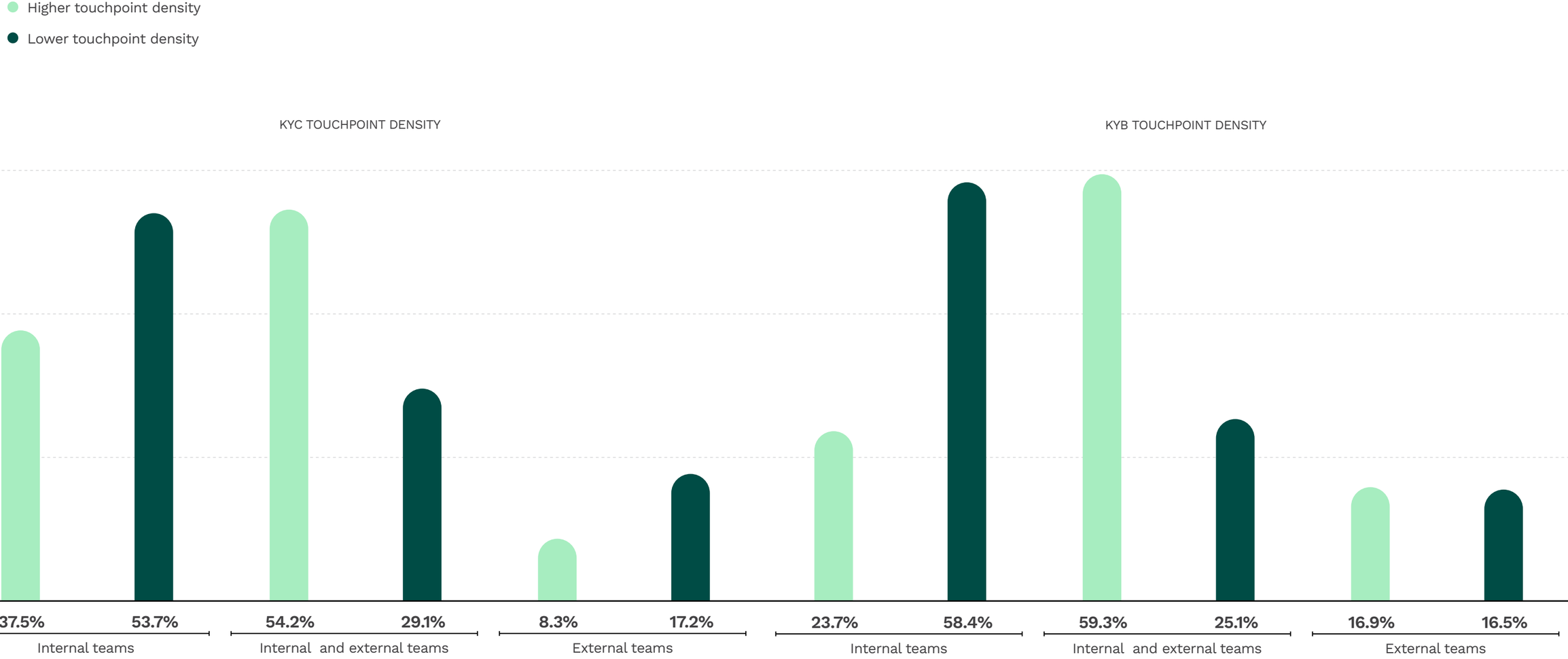
As companies use identity checks across more workflows, they are much more likely to run KYC/KYB through a hybrid operating model combining internal teams with external partners.

In the higher-density group, internal and external teams are the primary manager for a majority of firms (KYC: 54.2% vs. 29.1% in lower density; KYB: 59.3% vs. 25.1%). By contrast, lower-density firms are more likely to keep responsibility primarily in-house (KYC internal only: 53.7% vs. 37.5%; KYB internal only: 58.4% vs. 23.7%).

As the number of identity checkpoints grows, managing them tends to shift from a single team function to a coordinated model, suggesting that higher-density programs require more cross-team coverage and specialized support to operate consistently.

FIGURE 8:

Primary manager of KYC/KYB operations



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

Broader workflow coverage aligns with easier KYC/KYB operations.

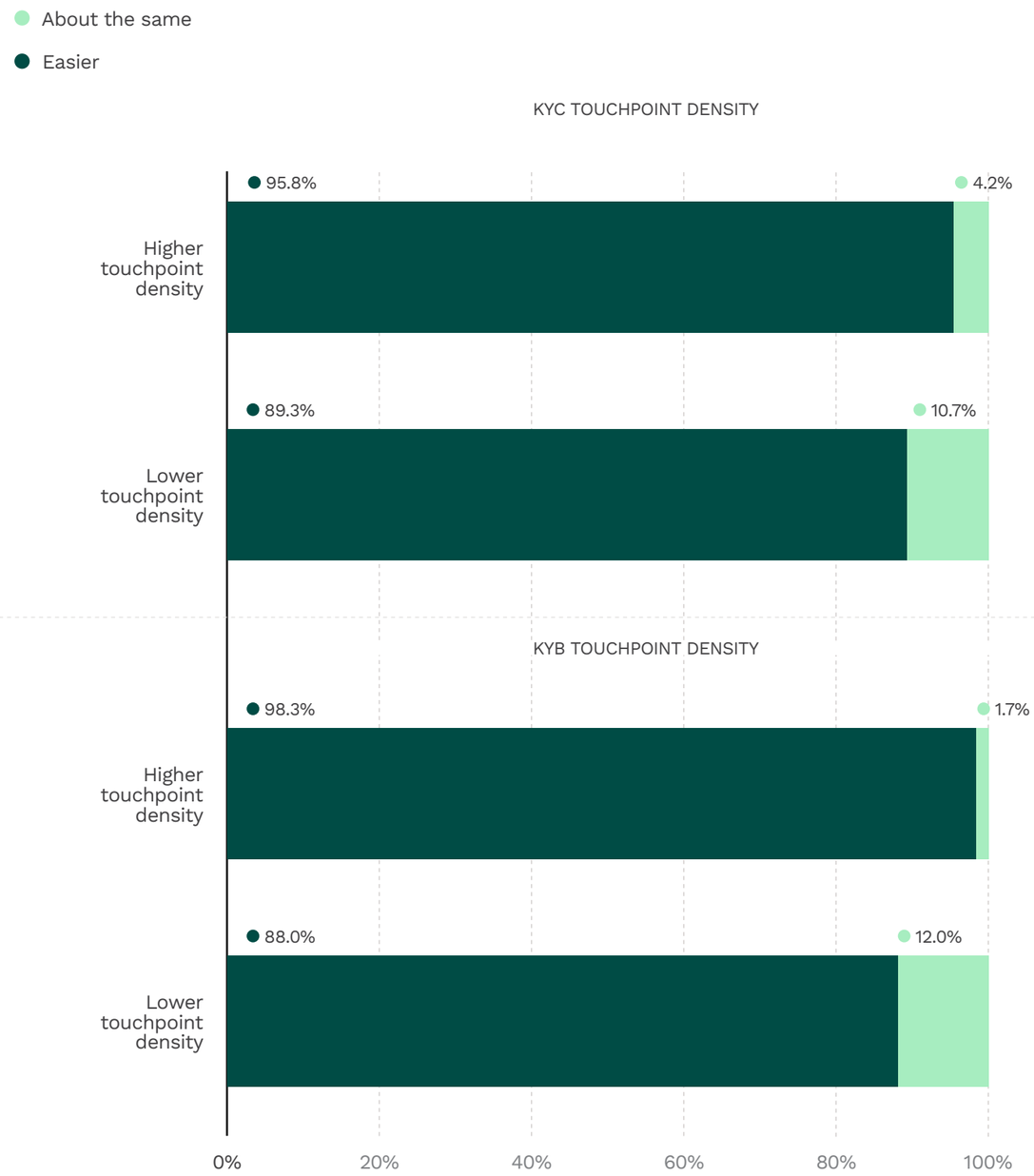
Most firms report that KYC/KYB has become easier over the past 12 months. Improvement is strongest among firms running identity checks across five-plus workflows: 95.8% say KYC is easier, and 98.3% say KYB is easier. Firms with checks in fewer workflows are more likely to report no change (KYC: 10.7%; KYB: 12%).

98.3%

of firms running KYB checks across five or more workflows say **verification has become easier over the past year.**

FIGURE 9:

Change in KYC/KYB difficulty over time



Source: PYMNTS Intelligence
Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk
N= 350; fielded August 1, 2025, to September 10, 2025

March 2026

Digital Identity Framework

Identity at Scale:

Where KYC/KYB Touchpoints Create (or Contain) Agent Risk

PYMNTS INTELLIGENCE | Trulioo

Methodology

Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk is **based on a survey of 350 companies conducted from August 1, 2025, to September 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, the United Kingdom, the 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.**

Lynnley Browning
Managing Editor

Yvonni Markaki
SVP, Head of Analytics

Matthew Albrecht, Ph.D.
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

Identity at Scale: Where KYC/KYB Touchpoints Create (or Contain) Agent Risk 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.