NICE Actimize

White Paper

Omni-Channel Authentication:

A Unified Approach to a Multi-Authenticator World

Overview

From “selfie authentication” to behavioral biometrics, Financial Institutions are rapidly investing in innovative authentication methods across their banking channels.

With the proliferation of new authentication methods, FIs often find themselves running disparate tools without a unified cross-channel management or orchestration approach. These siloes can lead to a series of problems, including poor customer experience, ineffective authentication and challenged fraud prevention strategies.

The answer is not to avoid authentication innovation, but rather to create an orchestration strategy, which manages policy and execution for multiple authenticators across the contact center, digital channels, ATMs and the branch.

The results of this NICE Actimize 2017 Omni-Channel Authentication Survey show that FIs are largely ready to transform the way they manage and execute customer-facing authentication across their organizations. The drivers behind this change tell a new story of the role of authentication in the FI.

NICE Actimize

Contents

NICE Actimize

Why an Omni-Channel Authentication Survey?

Authentication innovation is still in its infancy, and most FIs are still combining more traditional passwords and PINs with cutting edge biometrics or contextual decisioning methods. The combination brings new capabilities to multi-factor authentication, but doesn't necessarily produce the best possible results.

FIs commonly report that their users face inconsistent customer experience across channels—for example consumers enjoy simple, password-free facial biometrics in the mobile app while fumbling over passwords and even knowledge-based authentication (KBA) questions in the online channel. Things only worsen in the contact center where consumers often have completely unique authentication methods.

Beyond inconsistent user experience, a lack of authentication orchestration can also lead to unnecessary customer challenges and friction, which results in frustrated calls to the contact center and ultimately an unnecessary drain on overall FI operations.

We set out to understand the challenges of silo-ed cross-channel strategies, as well as the potential solutions.

Objectives of this survey include:

Quantify the need for omni-channel authentication orchestration

Identify necessary elements of an omnichannel authentication strategy

Determine metrics for a successful omnichannel authentication orchestration strategy

Define the relationship between authentication orchestration and fraud prevention solutions

Methodology: Global Presence and Diverse Stakeholders

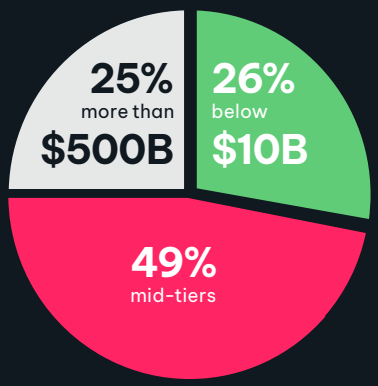
The 2017 Omni-Channel Authentication survey was developed by NICE Actimize and PwC in March 2017 and conducted through a third-party survey firm with promotions through Finextra, LinkedIn, and user/ client communities of both NICE Actimize and PwC.

Over a one-month period, this survey was answered by 75 experts, with more than half representing retail banking and the rest spread rather evenly across corporate and private banking environments.

75
EXPERTS

OVER 1 MONTH PERIOD

Respondents represent a global view with 38% serving in active roles in Europe, 20% in North America, 13% in Asia Pacific and 14% claiming global roles.



Additionally the survey represents a range of FI sizes with the highest concentrations in the very largest and the very smallest organizations. Of respondents, 25% represented global tier 1 organizations with assets of more than $500B while 26% represented organizations with assets of below $10B. The other 49% were equally spread across the mid-tiers.

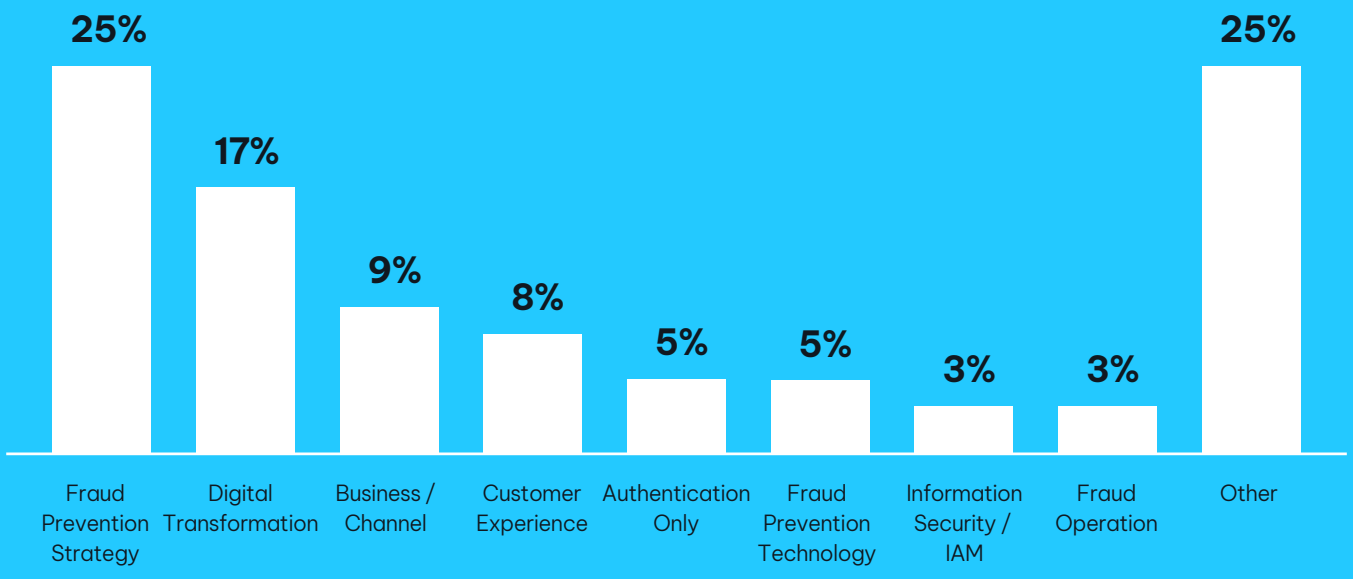
Respondents: Interest in Omni-Channel Authentication beyond Security or Fraud Prevention Teams

Customer-facing authentication is often linked to fraud and Information Security groups, but we found there are a wider set of FI experts when it comes to interest in a cross-channel orchestration strategy.

About a third (33%) of the survey's respondents are responsible for fraud strategy, technology or operations, while another third (34%) are responsible for a combination of channel management, digital transformation and customer experience. The breakdown of respondents is the first indicator that omni-channel authentication orchestration is about a lot more than improved security.

1/3 of respondents are responsible for fraud prevention, while 1/3 are responsible for digital transformation, channel and customer experience

Which of the following best describes your primary role?



NICE Actimize

Key Findings: FIs Beginning the Journey to Authentication Orchestration

At a high level, the results of this survey paint a key narrative—the age of omni-channel authentication is upon us and it will be driven as much by the need to enhance customer experience and enable digital transformation as it will be about improving security and fraud prevention measures.

The following are some key trends that emerged from our results:

FIs are preparing for omni-channel authentication orchestration:

Today, many FIs are assessing their current authentication programs to determine gaps and prepare for cross-channel authentication management and orchestration.

Digital transformation and customer experience are central drivers of change:

Digital transformation—and resulting improved customer banking experience—are as important to omni-channel authentication strategy as fraud prevention or security. As such, FIs will measure the success of their authentication strategies partially through customer experience metrics.

Bridging authentication and fraud strategies:

FIs are seeking the ability to more easily integrate risk and fraud analytics into their authentication strategy, where today they're largely siloed.

63%

will assess current authentication strategies to identify needs for omni-channel authentication strategy (30% have completed assessment)

61%

will invest in an omni-channel authentication orchestration solution within 12-18 months

28%

have the ability to manage all authenticators across all channels today

83%

say customer experience is a key business driver in omni-channel authentication management investment

58%

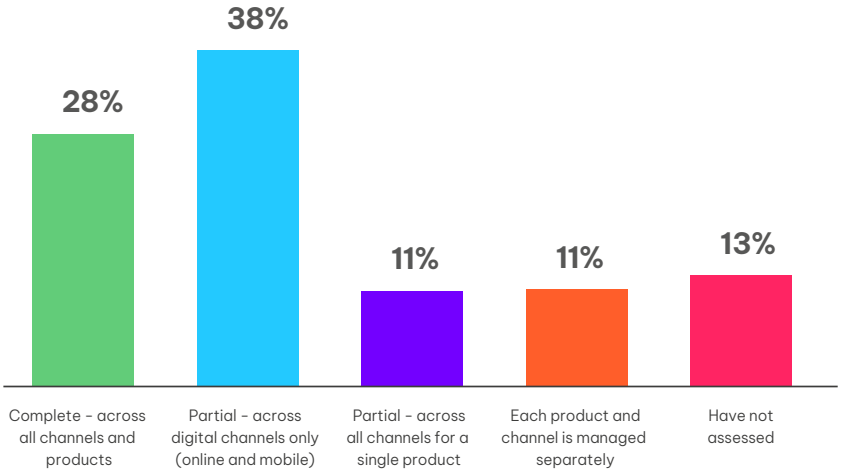
will integrate fraud and risk data into omni-channel authentication orchestration decisioning

The State of Omni-Channel Authentication Strategy

Today about a quarter (28%) of Financial Institutions have implemented unified cross-channel authentication management, most of these are organizations with assets of less than $20B, while the large majority (49%) have partial cross-channel coverage

That partial coverage can entail shared orchestration across some channels for many authentication products, or it can mean a unified approach to managing a single authenticator across multiple channels. Smaller organizations might have a smaller authentication products portfolio or operate across fewer channels and thus reach unified cross-channel authentication management before larger organizations.

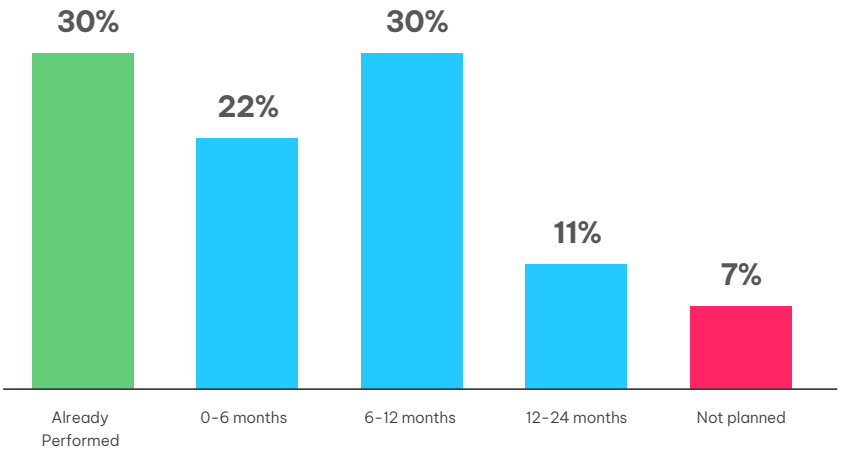
What is the extent of your ability to manage your authenticators across different channels from a centralized system?

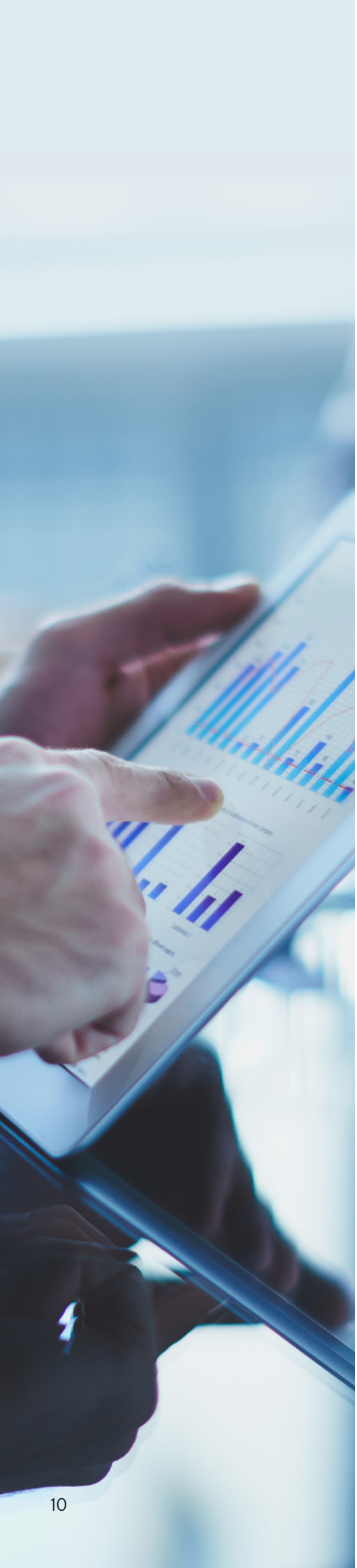


This lack of unified coverage across channels is likely to change shortly.

More than half (52%) of our survey's respondents will assess their authentication strategies in the coming year to begin the process of better aligning their authentication methods across channels. Meanwhile almost a third have already begun the process.

In which of the following timeframes does your organization plan to hold an authentication program assessment to better align silo'd policies, processes, and technologies to an omni-channel framework?

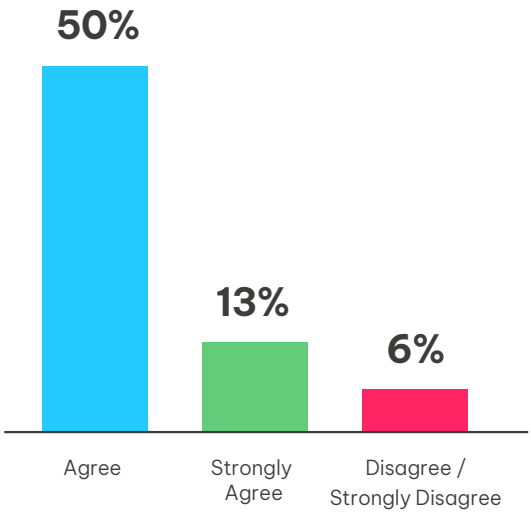




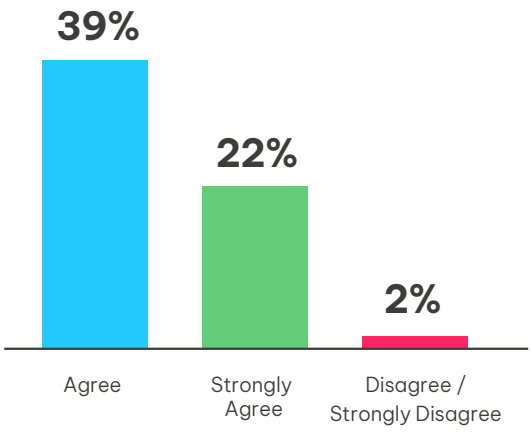
The State of Omni-Channel Authentication Strategy

Implementation of an authentication orchestration will follow shortly after this assessment with 61% of respondents saying they will invest in omni-channel orchestration within 12-18 months.

We will invest in aligning our contact center and digital channels authentication



We will invest in an omnichannel authentication orchestration solution



NICE Actimize

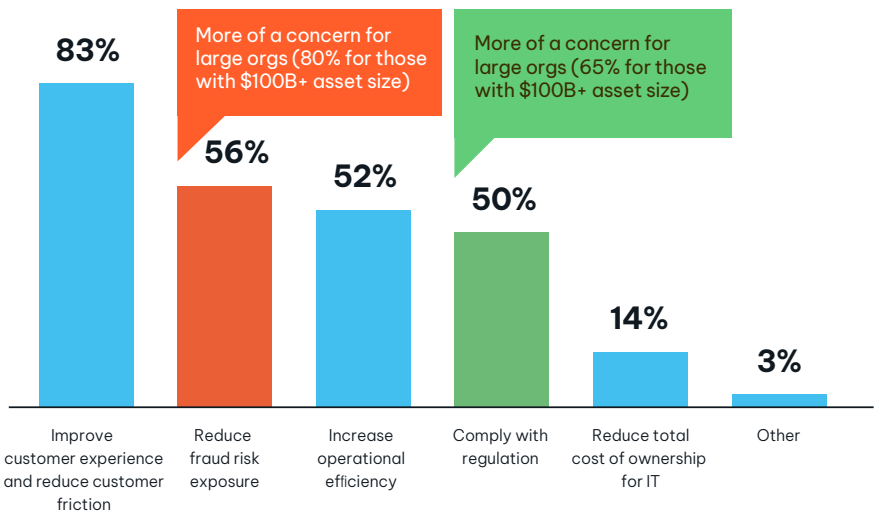
Driving the OmniChannel Authentication Investment: Customer Experience & Fraud Prevention

Authentication is often seen as the first line of defense in preventing fraud attacks—yet fraud reduction won't necessarily be the key driver to an investment in omni-channel authentication management. In fact, survey respondents as a whole point first to improved customer experience as the leading investment driver (80%) with fraud prevention and enhanced operational efficiency rank second (56%) and third (52%) as drivers respectively. Among larger FIs with assets overs $100B, reducing fraud and improving customer experience weighed out more equally as drivers, with 80% of respondents naming both equally as central drivers.

Why does customer experience play such a central role in authentication orchestration? For one, we will see in this report that customer authentication experience is cumbersome and frustrating for customers in large part due to a lack of unified authentication management. As a result, most authentication orchestration solutions aim to equally improve customer experience and reduce attacks by enabling better challenge decisions, which are based upon risk and customer preference. The idea is to challenge the riskiest, while easing up on safer users.

Among larger FIs with assets overs $100B, reducing fraud and improving customer experience weighed out more equally as drivers, with 80% of respondents naming both equally as central drivers.

What are key business drivers considered when determining omnichannel authentication strategy in your organization?



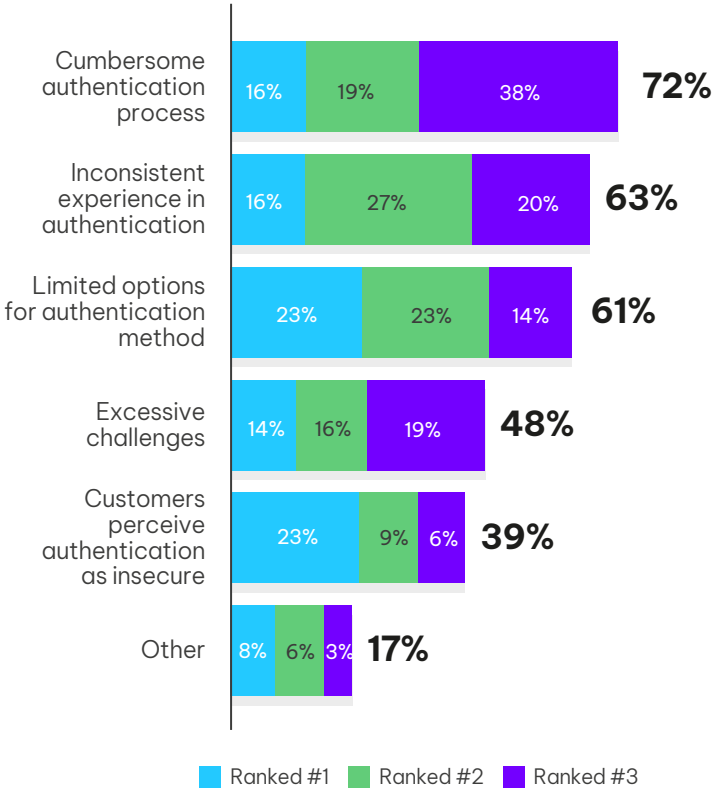
Authentication: A Myriad of Customer Experience Woes

Poor customer authentication experience is so common that it has generated social media memes and late night TV jokes. Just about every consumer has been asked that impossible knowledge-based authentication question—like, "What car did you own in 1991?"

So first and foremost, improving customer experience means reducing friction in the form of excessive authentication challenges and unnecessary calls to the customer.

But FIs see challenges beyond basic friction. They have a problem with consumers facing inconsistent experiences as they engage across channels (63% ranked as a top three challenge), where, for example, a customer uses simple facial biometric authentication in the mobile channel only to be asked for a password and a PIN online an hour later. Additionally, in the age of authentication innovation, consumers want preference in authentication type, but FIs still don't believe they are able to offer enough choice in authenticator (61% ranked this as a top three challenge).

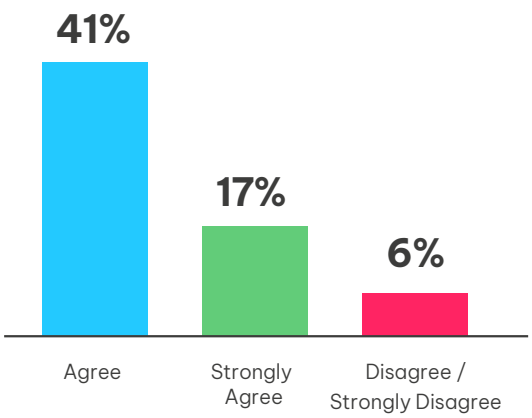
What is biggest challenge your authentication strategy poses to your customers? (Top three challenges ranked)



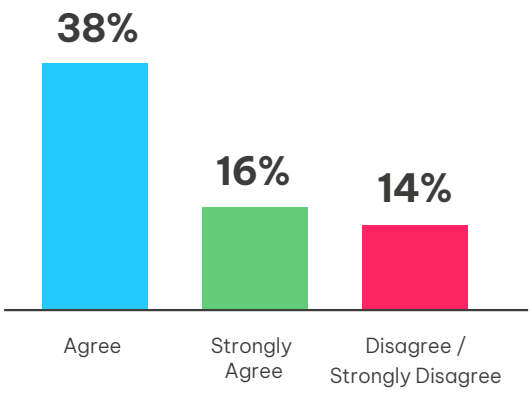
Bridging Fraud Detection and Authentication Orchestration

Integrating historic fraud and authentication data provides a wider view of the customer's typical banking journey and transactional behavior—enabling orchestration solutions to make more nuanced decisions on how and when to challenge customers. For example, integrating fraud and authentication history means the use of contextual data, such as device, locations and relationships, as well as transactional history, in every authentication challenge decision.

We will integrate fraud risk data for making authentication decisions



We will consider customer's authentication history when evaluating a fraud risk score



Nearly
60%

of respondents will invest in orchestration solutions which integrate fraud or risk data and authentication history into the challenge decisioning process.

Elements of an Authentication Orchestration Strategy

As FIs look to invest in authentication orchestration in the next 18-24 months, they'll seek features ranging from contextual, non-intrusive authentication methods to the ability to measure the success of their authenticators. Some of the key areas of investment include:

Agile Authentication Policy and Strategy:

59% of FIs will invest in authentication management solutions which enable them to nimbly alter policy rules that guide challenges, step-ups and authentication execution. This kind of investment is especially important as FIs prepare to support emerging faster payments, which are likely to attract rapid fraud spikes and/or shifts in consumer use. It is important to be able to easily changeup strategy on who and when to challenge when fraud is moving quickly.

Measuring Authentication Efficacy:

As FIs transition to an omni-channel authentication approach, one key element will be to measure how effective individual authenticators are. In the survey, 55% of respondents said measurement of authenticator performance is a key element of an orchestration strategy.

While success metrics may focus on reduction of fraud, it's just as likely they'll measure achievement based on improved customer experience—for example, reduction of unnecessary challenges or time spent in the system authenticating.

Efficacy is also likely to be measured understanding impact of authentication on the operations team—for example, less time managing calls about unnecessary challenges, and reduction in time spent managing conflicting alerts from disparate tools.

Enabling Customer Choice in Authentication:

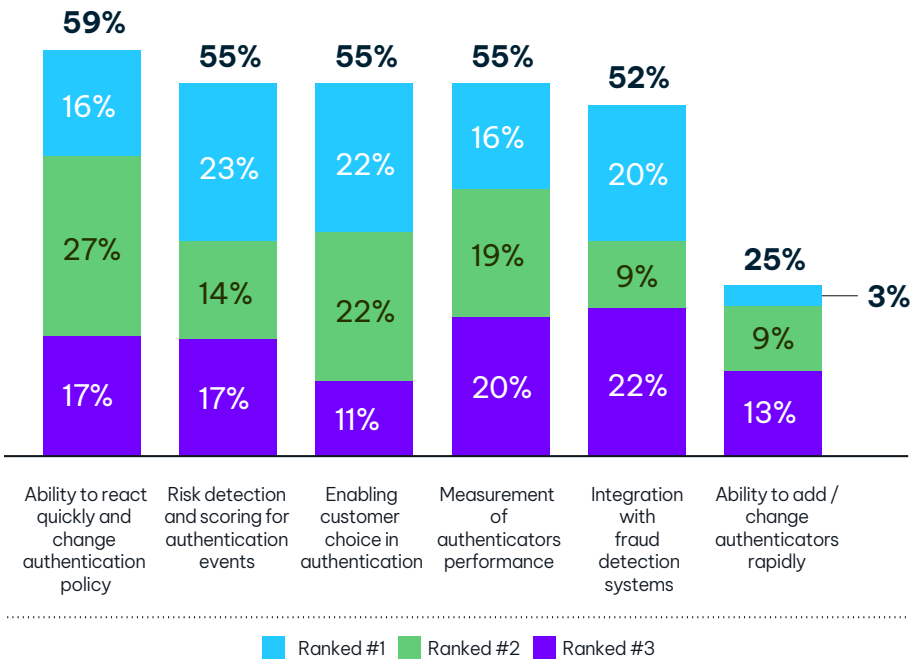
As FIs invest in a myriad of authentication methods, they'll want to support customer preference in authentication method. In some cases, customers will demand simple biometrics methods. Meanwhile others, will not necessarily feel secure with facial biometrics, for example, and they'll choose a more traditional authentication method. In the survey, 55% of respondents said customer enabling preference is a key element of an authentication orchestration solution.

63%

Continuous or Persistent Authentication Methods:

Survey results show that 63% of FIs will invest in continuous or persistent authentication methods, which rely on sophisticated analytics to verify consumer identity and assess risk without requiring active authentication. Continuous authentication can use a wide range of techniques from behavior biometrics to device analysis. The investment reduces friction by both cutting active authentication and producing fewer unnecessary challenges—lending itself directly to the key objective of improved customer experience.

How important are the following elements to an authentication orchestration solution? (Top three elements ranked)

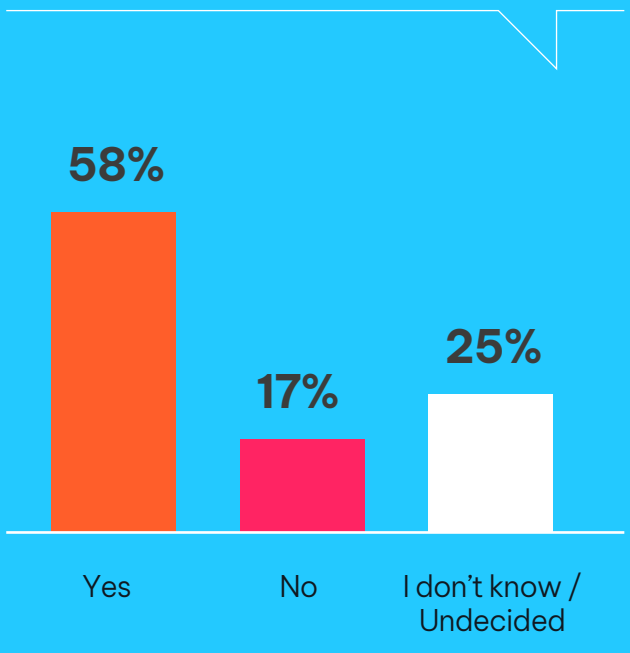


PSD2: A Driver for Authentication Orchestration

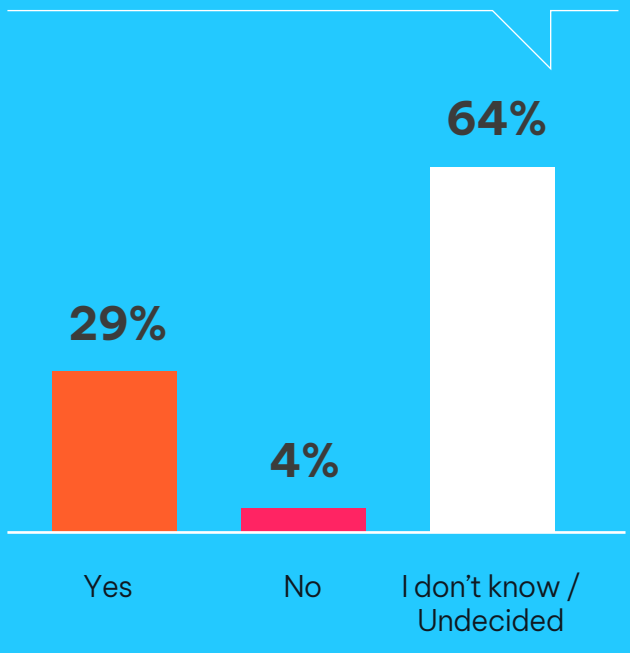
Nations across Europe are preparing to comply with Payment Services Directive 2 (PSD2) regulations from the European Banking Authority (EBA), which require them to provide public APIs to thirdparty Fintech providers and aggregators. In complying, many FIs will find the need to invest in new authentication methods and orchestration. Under PSD2, "Strong Customer Authentication" (SCA) rules require FIs to implement twofactor authentication for most payment transactions (and some non-monetary events)—and this will drive investment in new authenticators.

PSD2 rules have swung the pendulum on allowing riskbased decisioning as part of SCA. In early days, the use of risk-based analytics to decide on authentication challenges was prevented, but now regulation has been altered to allow exemptions depending on transaction risk. Nevertheless, only 30% of respondents say they will use this exemption; meanwhile a whopping 67% are undecided.

Will Strong Customer Authentication (SCA) requirements under Revised Payments Service Directive (PSD2) drive investments in new authentication methods?



Are you planning to use the risk based authentication exemption for "Strong Customer Authentication" detailed in the final Regulatory Technical Standards (RTS) draft?

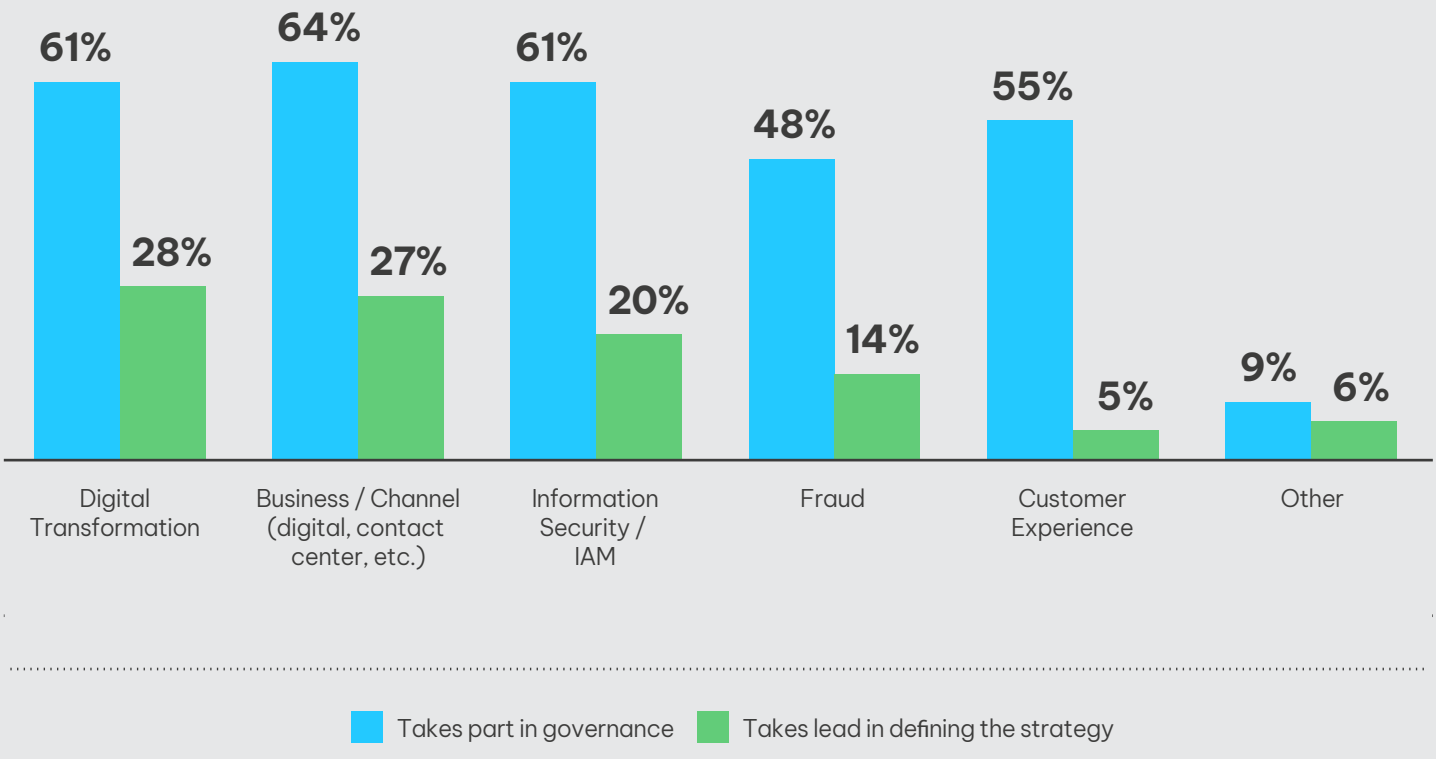


Who Will Define and Govern Omni-Channel Authentication?

Since omni-channel authentication will be largely driven by customer experience, digital transformation and fraud prevention in equal parts, it makes sense that the stakeholders responsible for implementing and managing such a strategy would be diverse.

According to the survey, omni-channel authentication strategy will be largely defined by groups responsible for digital transformation (28%), channel management (27%) and a smaller role for the fraud team (14%). Meanwhile, there will be a central presence in the governance of omni-channel transformation by digital (61%), channel (64%) and Information Security (61%) and customer experience (55%), with fraud playing a slightly smaller role (48%).

Parts of the organization that are involved in omni-channel authentication strategy



NICE Actimize

Preparing for the Age of Omni-Channel Authentication

This survey tells a clear story—in the coming 12-18 months, we'll see continued investment in authentication innovation and orchestration across FIs of all sizes. This strategy will have three clear objectives—improved customer experience, reduced fraud and by default, optimized operations. There will be nuances in how improved customer experience is defined. It may entail reduced unnecessary challenges, or customer preference in authentication type.

In all cases where FIs are seeking to strike the balance between reduced fraud and improved customer experience, they'll need an authentication orchestration system, which relies on rich data and advanced analytics to make dynamic decisions which reach across all channels and authentication methods

Authentication orchestration leading practices should include:

1 Risk-based authentication at log-in	An orchestration system should enable real-time, risk-based decisions at log-in, using dedicated analytics models which consider authentication and transactional risk history as well as a range of contextual data
2 Ongoing evaluation of risk throughout a session	Risk decisions for authentication shouldn't stop at the front door. An authentication orchestration system must continually evaluate risk throughout the customer session, continuing to make challenge decisions at each new event.
3 Nimble authentication strategy/policy management	An authentication orchestration solution should make FIs easily ready for change in fraud patterns and customer population changes. This will especially be true with the rise of faster payments and open banking. Solutions should provide a simple user interface to write, test and implement authentication challenge policy rules quickly.
4 Business intelligence reporting and insights to measure efficacy	FIs investing in brand new authentication orchestration strategies will seek success metrics. These metrics will be based on a combination of improved customer experience and fraud reduction. A best case scenario solution will include a visual analytics efficacy dashboard, displaying metrics on authentication tools and outcomes across channels.

Disclaimer:

PwC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. PwC gives no express or implied warranties, including but not limited to any warranties of merchantability or fitness for a particular purpose or use and shall not be liable to any entity or person using this document, or have any liability with respect to this document. This report is for general purposes only, and is not a substitute for consultation with professional advisors. It is intended for internal use only by the recipient and should not be provided in writing or otherwise to any other third party without PwC express written consent.

NICE Actimize

Know more. Risk less

info@niceactimize.com
niceactimize.com/blog
@NICE_actimize
/company/actimize
NICEactimize

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

niceactimize.com