FORRESTER®

The Identity Decisioning Imperative

Why Digital Banking Requires More Robust Identity Verification Tools

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY ALLOY | JANUARY 2022

Banks Need Greater Identity Insight Than Today's Tools Provide

Recent events have accelerated an already growing trend of customers seeking digital banking interactions. This shift has come with heightened opportunities and risks, and banks are finding it necessary to evolve their identity decisioning, i.e., the processes used to verify customers' identities during account opening, credit, and other identity scenarios, including those needed for AML and KYC requirements.[1] The challenge is that digital identities are nuanced. Banks are hard-pressed to find solutions to make faster, more accurate decisions that both catch fraud and reduce customer friction.

Alloy commissioned Forrester Consulting to explore identity decisioning at large financial institutions in the US. Through our survey of 100 senior leaders, we sought to understand the role an identity decisioning platform (IDP) can play in quickly and securely identifying suspicious actors without keeping out valid customers.

Key Findings

The threat of impostors has grown as consumers flock to digital banking channels. Most leaders cite that fraudulent applicants are increasingly outmaneuvering their identity decisioning tools.

An execution gap separates capabilities and aspirations. While automated identity decisioning is a top goal, the odds that a customer's identity will be verified automatically is akin to a coin toss.

An IDP can connect multiple data sources though a single API, allowing banks to significantly improve the number of customers that can be automatically decisioned quickly, accurately, and safely.

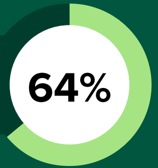
Overview
Situation
Approach
Opportunity
Conclusion

As Digital Banking's Popularity Grows, So Too Does Fraud Risk

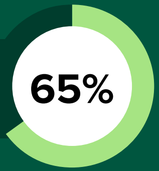
While digital banking has been on an upward trajectory for some time, the events of the last year and a half have accelerated consumers' migration to digital channels. As more customers become accustomed to online banking, and the fintech ecosystem evolves, expectations for fast and fully digital experiences are growing.

As customers shift to digital channels, fraudsters — as they always do — follow. Additionally, while the sophistication of their methods continue to grow, the exposure to fraud has increased, especially for banks that have technology stacks that can't keep up. Nearly two-thirds of decision-makers acknowledge that fraudsters are increasingly outmaneuvering their identity decisioning tools.

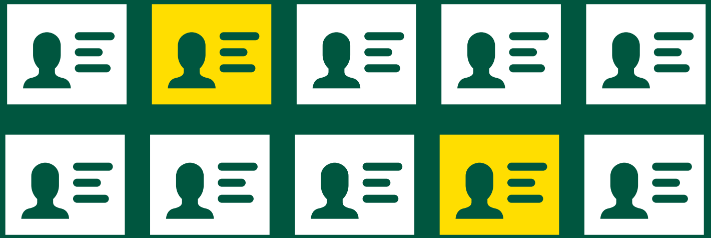
A growing proportion of our customers expect fast and fully digital experiences.



Increasingly, fraudulent applicants are outmaneuvering our identity decisioning tools.



Approximately 18% of accounts that are opened turn out to be fraudulent.



Base: 100 leaders at large financial services organizations in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

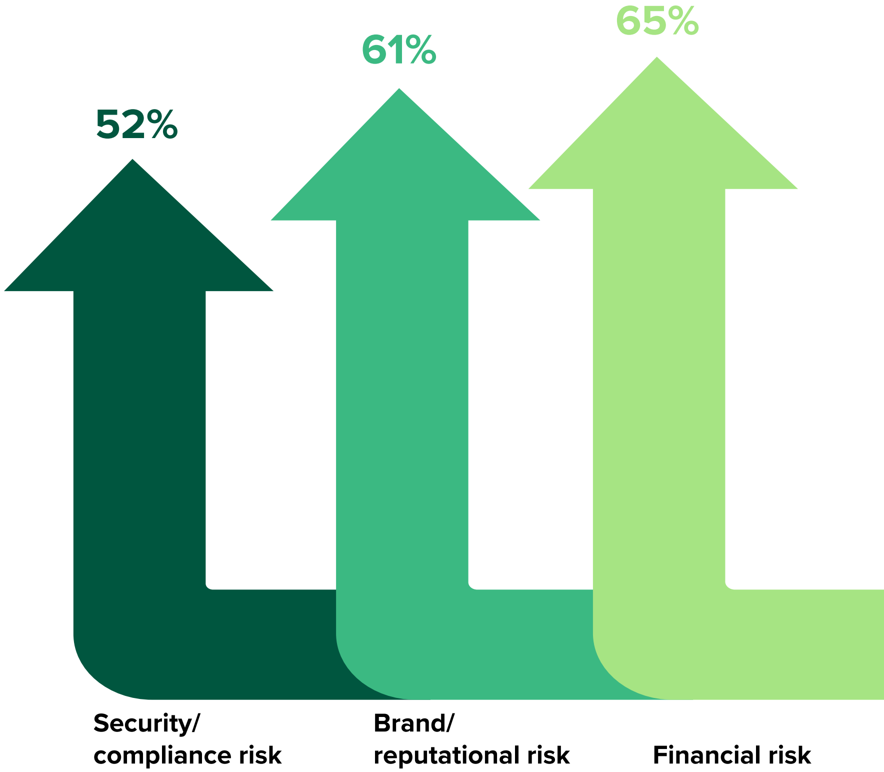
The Stakes For Effective Identity Decisioning Are Higher Than Ever

The rising threat of account takeover, identity theft, and privacy abuses has intensified the risk associated with having inadequate identity decisioning processes.[2] Respondents are concerned with several potential threats to their business, including: the financial losses resulting from an account opened in the wrong hands; the reputational hit and lost customer trust associated with stolen identities; and the impact of enforcement action and additional security requirements that would be needed if noncompliance was found to exist.

Given these risks, the majority of firms are making strong identity decisioning capabilities a priority, with about two out of three leaders indicating that COVID-19 has increased their organizations' commitment to identity decisioning enhancements.

65% are making identity decisioning improvements a priority.

Percent Indicating That The Risk Of Ineffective Identity Decisioning Is Growing



Base: 100 leaders at large financial services organizations in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

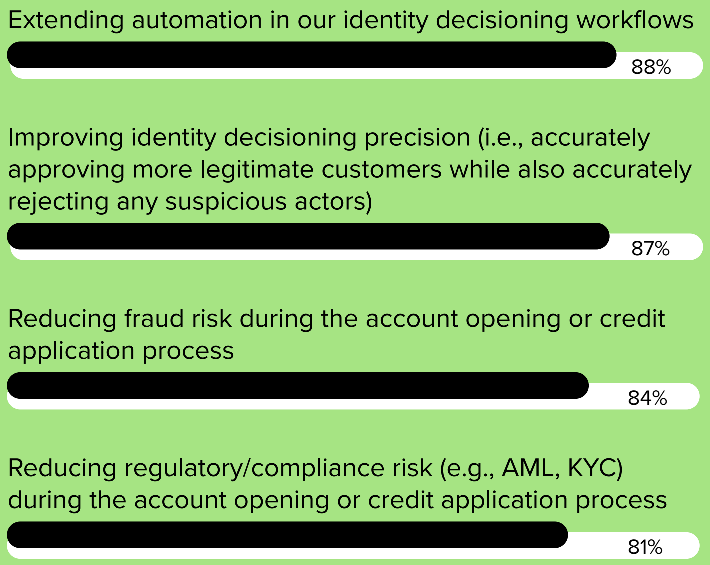
Overview
Situation
Approach
Opportunity
Conclusion

Capabilities And Aspirations Differ

Firms are focused on several near-term goals to make their identity decisioning ambitions a reality. Given consumers' demand for fast digital experiences, it's not surprising that extending the level of automation within identity decisioning workflows is at the top of their list. However, speed cannot come at the cost of accuracy. As such, a similar proportion say that improving identity decisioning precision is important. Also, over 80% are looking to reduce the fraud (84%) and compliance (81%) risk introduced in account opening and credit applications.

However, fewer than 40% are very confident in their ongoing ability to meet any of these goals. This sentiment holds true across product and client types. Fewer than half believe their organization is very effective at managing identity decisions made for checking/deposit account opening (45% for personal, 33% for small business) or credit applications (36% for personal, 35% for small business).

"How important are the following goals for your organization over the next 12 months?"



Fewer than 40% are very confident in their ongoing ability to meet any of these goals.

Base: 100 leaders at large financial services organizations in the US
Note: Showing "somewhat" to "very" important
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

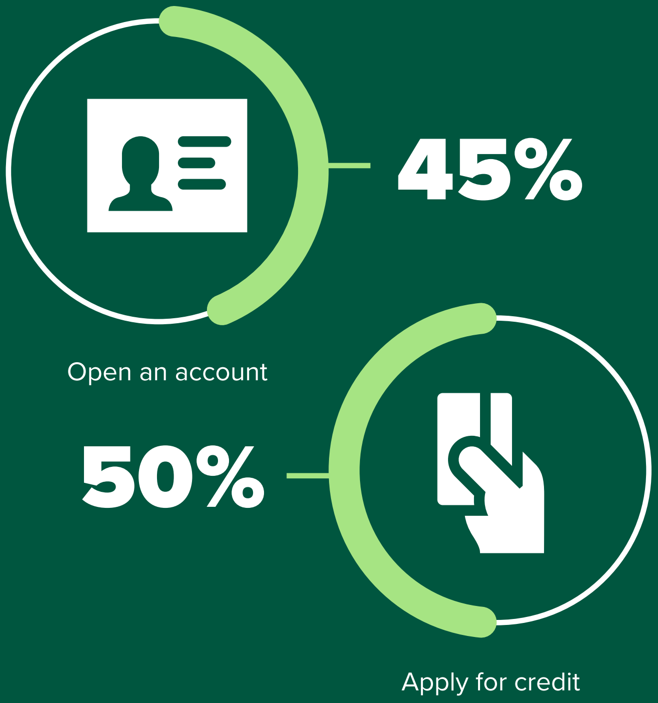
Overview
Situation
Approach
Opportunity
Conclusion

Automated Identity Decisioning Is An Uphill Battle

When it comes to opening an account or applying for credit, decision-makers recognize that slow and fragmented identity decisioning erodes both their customers’ and employees’ experiences. Understandably, 88% are looking to increase the end-to-end automation of their digital account opening and credit application processes. They realize that automated decisioning at this stage of the customer’s journey is vital to reducing the back-office burden for employees (83%) and improving customers’ impression of their brand (78%).

Despite the importance placed on providing automated, high-quality experiences, more work is needed to bring this vision to life. Only about half of customers who attempt to either open an account or apply for credit online have their identity automatically verified.

“What percent of customers who attempt to open an account or apply for credit online have their identity verified automatically (i.e., without exchanging physical documents or human intervention)?”



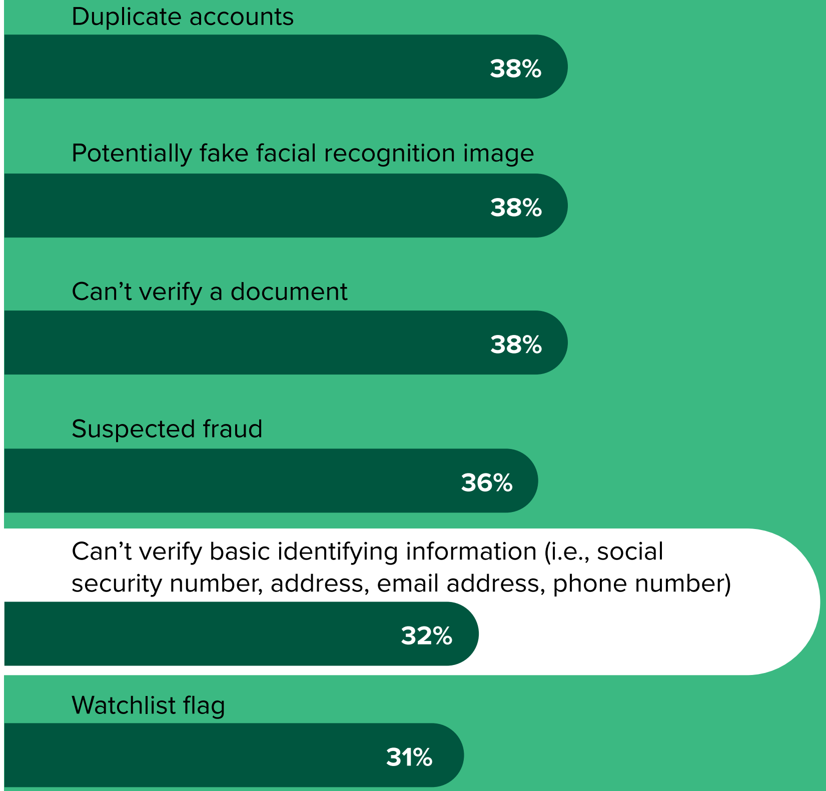
Base: 94 leaders at large financial services organizations in the US
Note: Showing median responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

Firms Are Bogged Down By The Basics

Duplicate accounts, dubious facial images, or the inability to verify a document commonly trigger manual identity verification. And often, these flags signal actual fraud.

However, 32% of banks commonly struggle to verify basic information such as a customer's address or phone number. While these flags may also be tied to fraud, they could be due to the customer having moved or changed their phone number. Sixty-two percent indicate that their systems return too many false positives like these. An inability to efficiently separate true customers from suspicious actors carries a high cost. Sixty-five percent express that their employees spend too much time on manual identity verification — time that might otherwise be spent on strategic work. And 61% say their lack of agility in managing fraud and identity processes is limiting their growth, which leads to lost revenue opportunities as customers that should have been converted await human intervention.

Common Reasons Identity Decisioning Workflows Require Manual Intervention



Base: 100 leaders at large financial services organizations in the US
Note: Select all that apply
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

Overview
Situation
Approach
Opportunity
Conclusion

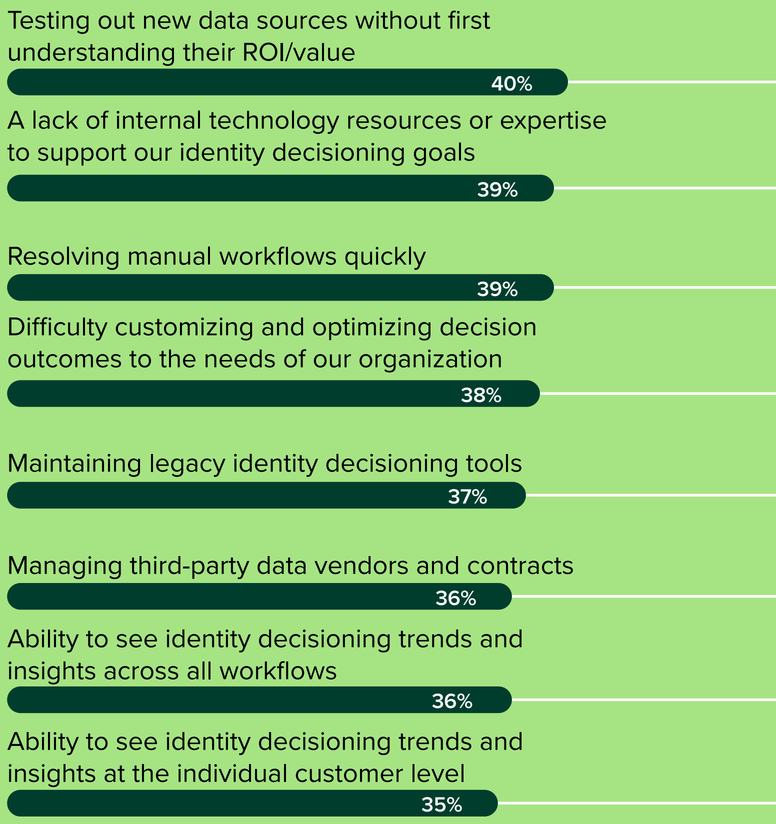
Complexity Is Inhibiting Success

The fragmented nature of customers' digital identities means that using one or two data sources for identity validation is no longer sufficient. Increasing the number of data sources boosts decision accuracy, but it also adds a complexity that most organizations are ill-equipped to handle. The need to continuously test new data sources is a top challenge. Consider that beyond identifying the right data sources, a bank would also need to integrate, test, adjust (e.g., make rule changes), maintain, and oversee the vendors associated with them.

Making matters worse, firms lack the requisite technology resources and expertise to manage the growing number of data sources, disjointed workflows, and legacy tools that are all unintuitively patched together. As a result, decision-makers lack visibility into identity decisioning trends and insights, making it difficult for them to optimize decision outcomes.

56% agree the number of data sources needed for effective identity decisioning is proliferating.

"What are your organization's top identity decisioning challenges?"



Base: 100 leaders at large financial services organizations in the US
Note: Select up to the top five; showing top challenges
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

IDP Adoption Is Top-Of-Mind For Most

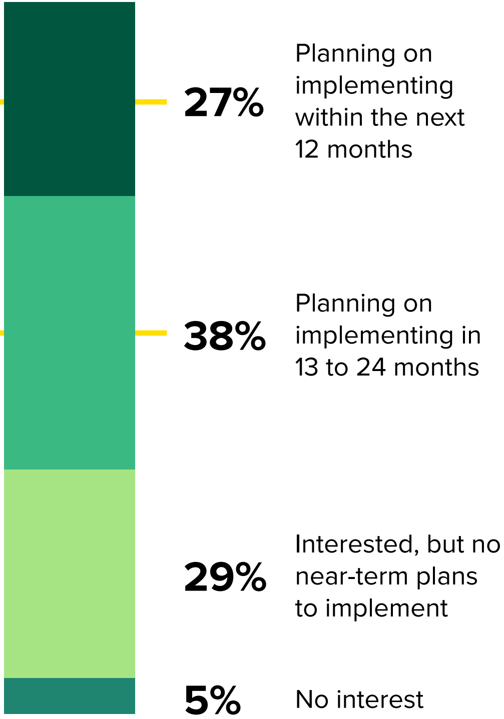
About half of firms are using entirely manual (13%) or in-house (36%) tools that patch together various data vendors to verify identities. These methods cannot keep pace with digital banking demands. Compared to those that incorporate purpose-built solutions from outside vendors, those relying solely on in-house or manual tools are more likely to: say they spend too much time manually verifying identity information (71% vs. 59%); describe the collection of tools that make up their identity decisioning portfolio as complex (67% vs. 53%); and verify even basic information manually (37% vs 27%).

A leading segment (9%) have embraced an IDP which can connect multiple data sources though a single API, allowing users to build decision workflows for fraud, AML, KYC, and other identity and risk scenarios in an automated fashion. The value of IDPs are not lost on decision-makers: 94% of those who have yet to adopt an IDP report near-term plans or interest.

65% of those who have not already adopted an IDP plan to adopt within the next 12 to 24 months.

"Which of the following best describes your organization's IDP adoption plans?"

(Select one; asked of those who do not already have an IDP)



Base: 91 leaders at large financial services organizations in the US
Note: Percentages do not add up to 100% due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

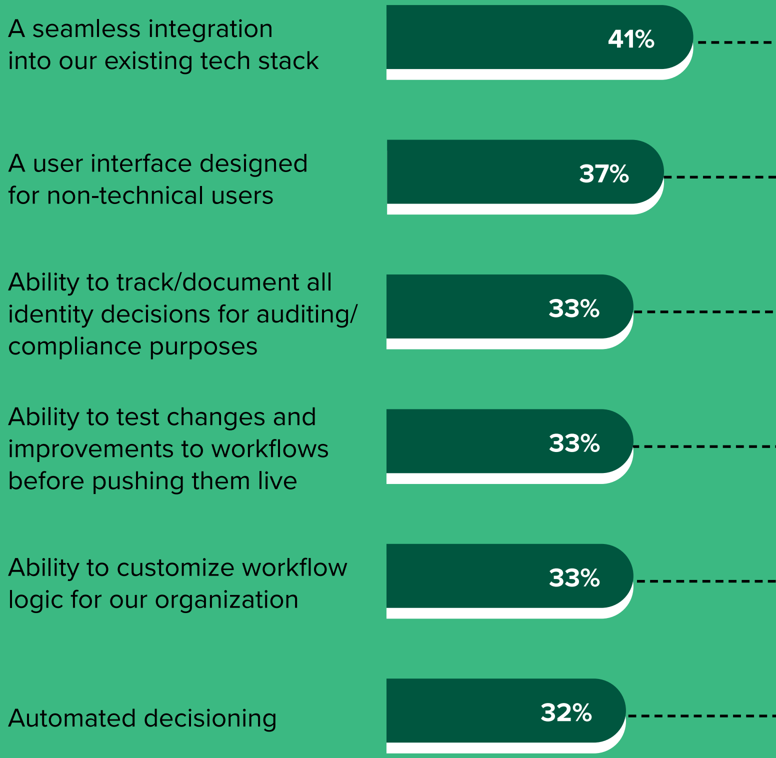
Overview
Situation
Approach
Opportunity
Conclusion

Decision Makers Prioritize Interoperability And Ease-Of-Use In Decisioning Solutions

As organizations look to modernize their identity decisioning tools, they must evaluate which features are best suited to their needs. Given the complicated web of tools they are managing, it's no wonder that a seamless integration into a current technology stack without the need to rip-and-replace existing solutions is the most important consideration.

Many are also looking for an interface designed with non-technical users in mind. And a roughly equal proportion place the following abilities at the top of their feature list: easily document identity decisions for compliance purposes; test improvements to workflows before pushing them live; workflow customization; and automated decisioning. Organizations evaluating IDPs — especially those with disjointed tools that fail to deliver on their identity decisioning goals — should also give weight to this criteria.

"When evaluating identity decisioning vendors and solutions, which of the following would you consider important for them to offer?"



Base: 100 leaders at large financial services organizations in the US
Note: Select all that apply; showing top options
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

Overview
Situation
Approach
Opportunity
Conclusion

Credit Applications And Account Opening Are Just The Tip Of The Identity Iceberg

Over two-thirds of decision-makers recognize that identity and fraud risk are not one-time, static concerns restricted to account opening and credit application processes. Eight out of 10 respondents indicate that developing an evolving, holistic view of customers' identities is important to their organization.

This means that ongoing transaction monitoring which spots high-risk or unusual activity, once either an account is opened or credit is extended, is an important part of an identity decisioning strategy and solution. In fact, the importance that decision-makers place on managing fraud risk with ongoing transaction monitoring (86%) is on par with the importance they place on managing fraud risk during account opening/credit application processes (84%). The same is true for compliance risk (85% for transaction monitoring versus 84% for account opening/credit applications).

68%

"Identity- and fraud-related risk extends far beyond the account opening/credit application process."

82%

"Developing an evolving, holistic view of customers' identities is important to our organization."

Base: 100 leaders at large financial services organizations in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

Overview
Situation
Approach
Opportunity
Conclusion

An IDP Can Promote Growth While Mitigating Risk

For too long, financial institutions have been forced to treat the accuracy, speed, and overall experience of their identity decisioning processes as seemingly opposing goals. A dedicated IDP can help organizations check off multiple boxes. Respondents agree that an IDP can automate and streamline identity decisioning to promote superior customer understanding and experiences during account opening and beyond. At the same time, it can support customers' growing desire to engage through digital channels in a way that is operationally efficient. And by providing a holistic view of identity, an IDP can better equip decision-makers to convert more legitimate applicants and restrict fraudulent ones quickly and accurately.

Top IDP Benefits Realized Or Expected

(Showing top five)

- Increased proportion of customers using digital channels
- Reduced regulatory/ compliance risk
- Improved ability to develop a holistic view of customers' identities
- Greater operational efficiencies
- Greater end-to-end automation of digital account opening/credit origination processes

Base: 100 leaders at large financial services organizations in the US
Source: A commissioned study conducted by Forrester Consulting on behalf of Alloy, November 2021

Conclusion

Identity decisioning tools are more important than ever. The risk of imposters and the opportunity from digital consumers means:

Banks must modernize their decisioning tools. Identity verification methods have not kept pace with the complexity of customers' lives and the sophistication of fraudsters. Outdated tools present financial, brand, and compliance risks.

Improving customer experience is crucial. On average, the identities of about half of digital customers is still decided through human intervention. This erodes customer confidence in digital experiences and is inefficient.

IDPs can close the execution gap. An IDP can significantly improve the number of customers that can be automatically decisioned. It can also support an evolving, holistic view of customers' identity, which most say is important to their company.

Project Director:

Sophia Christakis,
Market Impact Consultant

Contributing Research:

Forrester's Digital Business
Strategy research group

Methodology

This Opportunity Snapshot was commissioned by Alloy. To create this profile, Forrester Consulting supplemented existing Forrester research with a custom survey administered to 100 leaders at large financial services organizations in the US with knowledge into their organizations' compliance/ risk technology, digital banking strategy, and/or account opening/credit application processes. The custom survey began in October 2021 and was completed in November 2021.

ENDNOTES

[1] AML: anti-money laundering; KYC: know your customer.

[2] Source: "How Financial Services Firms Can Better Protect Customers," Forrester Research, Inc., May 13th, 2021.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

SECTOR	
National bank	**42%**
Regional bank	**37%**
Community bank/ credit union	**20%**
Online or pure play lending institution	**1%**

ASSETS UNDER MANAGEMENT (USD)	
$25B to under $50B	**14%**
$50B to under $100B	**31%**
$100B to under $250B	**34%**
$250B or more	**21%**

SENIORITY	
C-level	**14%**
Vice president	**42%**
Director	**44%**

DEPARTMENT	
Digital banking	**40%**
Product management	**34%**
Risk/compliance	**17%**
IT/security	**9%**

FORRESTER®