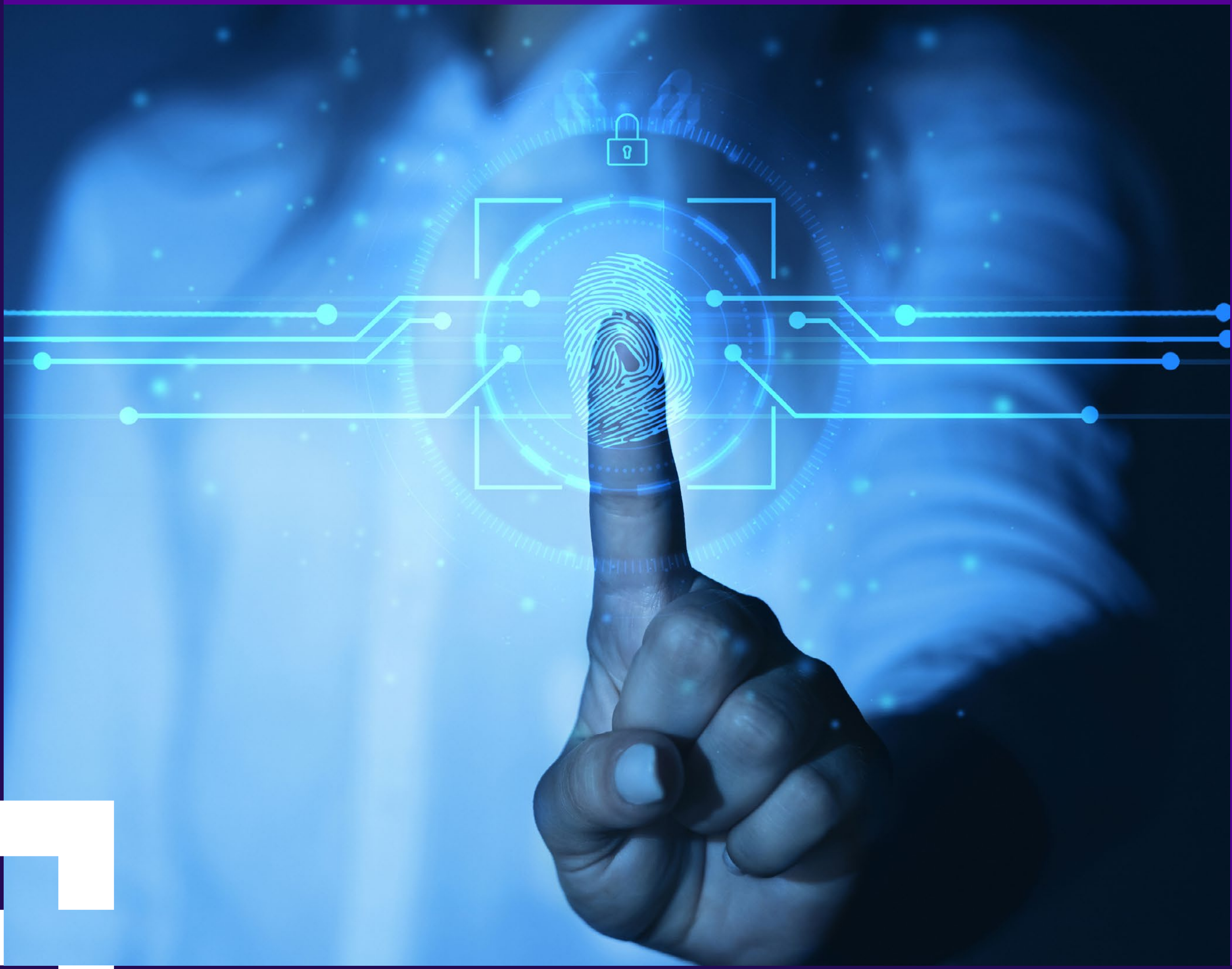
JAVELIN ADVISORY SERVICES | FRAUD MANAGEMENT

This report reprint is licensed by: Mitek

2023 Know Your Customer Solution Scorecard



javelin

JULY 2023

MEET THE AUTHOR

Suzanne Sando
Senior Analyst,
Fraud & Security

AUDIENCE

Vendors: KYC solution vendors, identity proofing vendors.

Financial institutions: AML/ BSA compliance managers, specialists in new-account fraud, product managers, and marketers responsible for KYC orchestration and deployment.

CONTRIBUTORS

Tracy Kitten
Director, Fraud & Security

Kevin Libby
Analyst, Fraud & Security

Overview

Know Your Customer (KYC) protocols are the bedrock of robust identity verification. Understanding at a granular level whom an organization is doing business with translates into a strengthened defense against identity fraud and, on a grander scale, is often the difference between detecting and preventing major financial crimes, such as money laundering or terrorist financing.

KYC is a standard that ensures financial institutions authenticate and verify their customers and members regularly. The three main components of KYC include a customer identification program, customer due diligence, and ongoing monitoring of a customer's account once it is established. For the purposes of this research, Javelin Strategy & Research analysts developed three weighted determinants that correspond across these components: Capabilities, Functionality, and Use Cases. Although Javelin analysts identified numerous vendors in the KYC space, this report reviews and ranks 16 of the vendors that cater to the U.S. market, particularly financial institutions. (Please refer to the report methodology for more information on inclusion and exclusion criteria.)

Primary Questions

- What technologies and features are available and considered critical for KYC vendors?
- What gaps in service must be filled to narrow the gap between the KYC Best in Class and Leaders and the rest of the market?
- How can KYC vendors better assist financial institutions with steady new-account growth and existing account monitoring while also ensuring that they remain compliant with Bank Secrecy Act (BSA) and USA PATRIOT Act regulations?

Table of Contents

Table of Figures

Executive Summary

LexisNexis Risk Solutions earns Best in Class overall. In addition to being named best in class, LexisNexis also achieved Leader rankings in the Functionality and Use Cases categories. LexisNexis offers a wide variety of customizations, individual user-facing features, and use cases for meeting KYC objectives that allow its financial institution customers to tailor their experiences to fit individual organizational needs within the product, thus making it easier to realize the true convenience and cost efficiency of a KYC solution.

Equifax Identity & Fraud Services, Alloy, and Mitek rank as overall Leaders. Equifax's, Alloy's, and Mitek's adoption of capabilities criteria evaluated by Javelin are all well above the average overall adoption rate (67%) across all vendors and often provide valuable and rare services, such as video KYC, something only offered by 38% of evaluated vendors. Additionally, all three were represented as leaders in individual categories: Capabilities (Alloy, Equifax), Functionality (Equifax), and Use Cases (Mitek).

Javelin evaluated providers across three sets of criteria: Capabilities, Functionality, and Use Cases. The category leaders are as follows:

Capabilities	Functionality	Use Cases
1 Alloy	1 LexisNexis Risk Solutions	1 Mitek
2 GBG	2 Equifax Identity & Fraud Services	2 LexisNexis Risk Solutions
3 Equifax Identity & Fraud Services	3 Experian	3 ComplyAdvantage

Identity fraud remains more than just a nuisance for consumers and financial institutions. Just over 15 million U.S. adults were victims of traditional identity fraud in 2022, with approximately $20 billion in traditional identity fraud losses[1]. Although those monetary losses decreased by 15% from 2021[2], the threat of identity fraud has certainly not been neutralized. Criminals are constantly shifting their attention to the newest exploitable digital banking or spending trend, so FIs are not necessarily safe from the threat of fraud, as former threats will eventually become hot with criminals again. Financial crimes, regardless of magnitude, continue to pose serious issues for consumers and organizations.

FIs must understand their customers' and members' sentiments regarding the collection, use, and possible storage of data for security purposes. The collection of personally identifiable information (PII) and other relevant consumer data is critical in the KYC process, at the initial account opening and for ongoing monitoring of account and transaction activity. To maintain steady new-account growth, FIs need to earn and preserve the trust of new and existing customers and members.

Responsible data sharing is not taken advantage of nearly enough. Only 63% of ranked vendors report validating consumer information against a data consortium among clients or external sources. Accessing data across sources doesn't mean the integrity of the data security is at risk, provided it is properly handled with the right access controls and defenses in place. The ethical use of a data consortium allows for a more accurate, highly confident, and data-rich resource for FIs to use in making decisions on new-account applicants and general account monitoring.

The adoption of dark web scanning is shockingly low, with only one-quarter of evaluated vendors offering this service. The only evaluated vendors to offer dark web scanning for shared or sold PII on malicious marketplaces are Alloy, Experian, Intellicheck, and Plaid. The adoption of such a valuable service should be significantly higher than 25%, and Javelin analysts urge vendors that do not currently employ dark web scanning to immediately integrate it into their existing services. This kind of information is extremely helpful to FIs and consumers in better assessing the risks of opening an account and applying fraud detection tools to attempt to prevent identity theft and identity fraud, or financial crimes and exploitation on an even larger scale.

Functional features like data visualization and report filtering are hard to find, though not necessarily essential to maintaining business. Although it may be worth the effort for KYC solution providers to look into offering integration with some of the more popular data visualization platforms or adding filtering functions, it's important to remember that data visualizations are a nice-to-have item but are understandably not as essential as the returned decision or score on a consumer.

The observance of ISO 20022 among ranked KYC vendors is still quite low, with just 31% of them currently adopting the new messaging standard. Initial migration to this new common-language payments messaging standard began in March 2023, and current messaging won't be retired until 2025[3]. Although the deadline is still quite far in the future, the earlier organizations ready themselves for full adoption, the better they can anticipate and resolve issues.

Recommendations

FOR VENDORS:

Prioritize nice-to-have features to elevate existing solution platforms. Much of what many KYC solutions already offer is required by law, so to remain competitive within the market of established solution providers, certain “extras” should be immediately added to the short-term road map of deliverables. These extras include dark web monitoring, KYC for business, human trafficking identification, money mule identification, report visualization tools, and assisted or fully automated filing of suspicious activity reports (SARs) and compliance reports.

Take advantage of a data consortium. Relying on a data consortium to further strengthen the result of identity verification does not mean an organization must sacrifice data integrity or security. It also doesn’t mean that more data, including PII, needs to be stored somewhere within a database to be useful.

Expand report and user-controlled functionality. While not the central mission of a KYC solution, reporting and interface functionality can often be a differentiator for an organization in the market for a new KYC solution. Features that boast a seamless experience for a vendor’s customers become the deciding factors when many other criteria for selecting a KYC solution hinge on features that ensure compliance with regulatory requirements, which are already available across every available KYC solution on the market.

Begin working on ISO 20022 migration immediately. To take advantage of data-rich messaging for cross-border and instant payments and better defend against identity fraud and financial crimes, FIs and KYC vendors alike must transition to the new standard sooner rather than later.

FOR FINANCIAL INSTITUTIONS:

Balance security with convenience. Securing accounts and ensuring consumer convenience don’t need to be mutually exclusive. Source a solution that maintains regulatory compliance, account security, and robust ID validation while also allowing consumers to navigate the account-opening process with ease and convenience. This can also translate into a better workflow for employees by removing unnecessary steps that cause issues for consumers or create lengthy manual reviews for employees.

Seek out KYC vendors that balance must-haves with nice-to-haves. Of course, it’s critical for a chosen KYC solution to provide the most accurate and swiftest results, but FIs should not forget about the nice-to-haves as well. If the returned data or user interface does not operate in a way that promotes efficiency and simplicity, the only outcome is more work for an FI employee to properly translate data into a practical and compatible format.

Be bold in asking about future developments when shopping around. The KYC space is constantly evolving to keep up with legal requirements and competition within the market. A discussion about forthcoming features and updates may become critical in the choice of a KYC solution.

The State of KYC

Know Your Customer (KYC) is the bedrock of robust identity verification for any financial services organization. Understanding at a granular level whom an organization is doing business with translates into a strengthened defense against identity fraud and, on a grander scale, is often the difference between detecting and preventing major financial crimes, such as money laundering or terrorist financing.

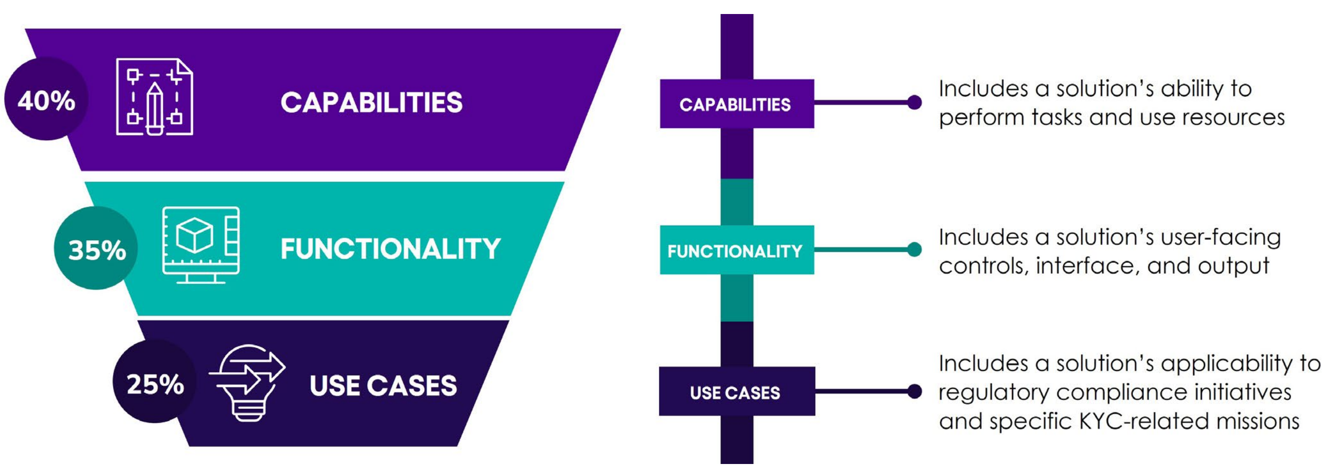
Javelin's Fraud & Security team defines KYC as the set of practices and technologies necessary to meet legal requirements outlined in the Bank Secrecy Act[4] and the USA PATRIOT Act[5]. For the purposes of this report, Javelin is employing a relatively broad definition that captures certain aspects of an organization's customer identification program, customer due diligence, and ongoing monitoring. However, the evaluation criteria rated by Javelin also include ancillary functions.

The KYC evaluation model created for this report is driven by three weighted determinants that correspond across these aspects: Capabilities, Functionality, and Use Cases. Within each category, Javelin analysts established weights for 100 criteria, based on each criterion's value and relative importance to its corresponding categories. Each category was then weighted to create an aggregate score and determine the ranking of every evaluated vendor.

Each evaluation category comprises weighted criteria deemed most necessary to meet basic regulatory requirements, along with the needs of organizations that employ a KYC solution for account opening and the ongoing monitoring of account and transaction activity. Although each category holds importance to the overall viability of a KYC solution, Javelin analysts weighed the Capabilities category heaviest, 40% of the overall aggregate score. Many core purposes and tasks fall under the Capabilities category. Following Capabilities in weighted importance is Functionality (35%), where organizations can tailor reporting outputs and controls to fit their specific business needs. Lastly, Use Cases closes out the KYC scorecard categories, weighing in at 25% of the aggregate score. This category holds plenty of valuable criteria, such as compliance with various global regulatory regimes, allowing for organizations to find a solution that meets its specific KYC-related objectives (see Figure 1).

Capabilities, Functionality, and Use Cases: Critical KYC Solution Components

Figure 1. Evaluation Criteria in Assessing KYC Solutions



Source: Javelin Strategy & Research, 2023

As identity fraud continues to make a significant mark on the livelihoods of consumers and the strength of financial institutions' business models and overall security postures, creating and maintaining an impenetrable account-opening and monitoring system for account and transaction activity is critical. According to Javelin's *2023 Identity Fraud Study: The Butterfly Effect*, just over 15 million U.S. adults were victims of traditional identity fraud in 2022, with approximately $20 billion in traditional identity fraud losses. Although those monetary losses decreased 15% from 2021, the threat of identity fraud has not been neutralized. Criminals are constantly shifting their attention to the newest exploitable digital banking or spending trend, so FIs are not necessarily safe from the threat of fraud, as former threats are likely to become hot topics for criminals again. Financial crimes, regardless of magnitude, continue to pose serious issues for consumers and organizations.

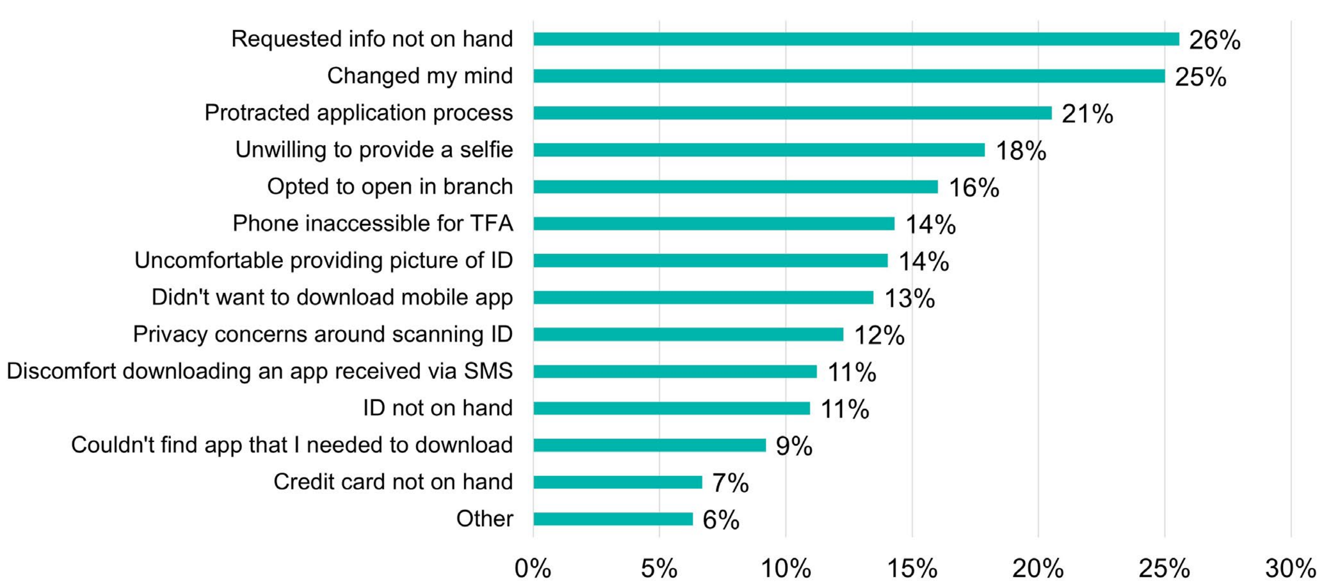
ROBUST AND RESPONSIBLE KYC ESTABLISHES TRUST WITH CONSUMERS

KYC isn't just for the benefit of business entities and organizations. When a financial institution demonstrates a vested interest in the security of its systems and protection for consumers against financial crimes, its customers and members experience an increased level of trust in the FI. This trust extends beyond established customers, stretching to prospective customers and members. If an FI has not established a convenient, secure account-opening process, application abandonment steps in and threatens the growth of new accounts.

Consumers will abandon their account-opening journey for a variety of reasons, but security-based concerns and lack of convenience were behind much of account-opening abandonment in 2022. Whether it's consumers' lack of confidence in the safety of taking a photo of a driver's license or passport (14%) or citing privacy and security concerns in scanning personal documents (12%), FIs are at risk of losing business if they don't immediately shore up the account-opening process with a robust identity fraud detection and prevention solution that also allows for a swift and simple process. And that begins with KYC.

Convenience and Security Concerns Stop Consumers from Opening New Accounts

Figure 2. Reasons for Consumer Application Abandonment in 2022



Source: Javelin Strategy & Research, 2023

Additionally, the collection of PII and other relevant consumer data is critical to KYC at the initial account opening and for purposes of ongoing monitoring of account and transaction activity. It's imperative that FIs understand their customers' and members' sentiments regarding the collection, use, and possible storage of data for security purposes.

Consumers are somewhat evenly split in how comfortable they may or may not be with their FI's collection of their data (see Figure 3). Nearly half of consumers are comfortable with their FI collecting personal (46%) and contact information (47%), while just over one-third (36%) are comfortable with their FI collecting information on their digital footprint. In the latter case, this could be due to a lack of understanding of what types of data points are included in a digital footprint, leading to a lower comfort level.

Consumers Are Somewhat Evenly Split In Collection of Information

Figure 3. Consumers' Level of Comfort with KYC Data Collection

	Extremely Comfortable	Somewhat Comfortable	Neutral	Somewhat Uncomfortable	Very Uncomfortable
Personal Information	18%	28%	22%	13%	20%
Contact Information	17%	30%	23%	16%	15%
Digital Footprint	14%	22%	24%	19%	20%

Source: Javelin Strategy & Research, 2023

For new-account growth to flourish, FIs need to be ready to explain what kinds of data are required and for what purpose if they are to secure and maintain the trust of new and existing customers and members. Much of this comes down to how compliant KYC solution providers are with various regulatory standards for consumer privacy and data collection and protection.

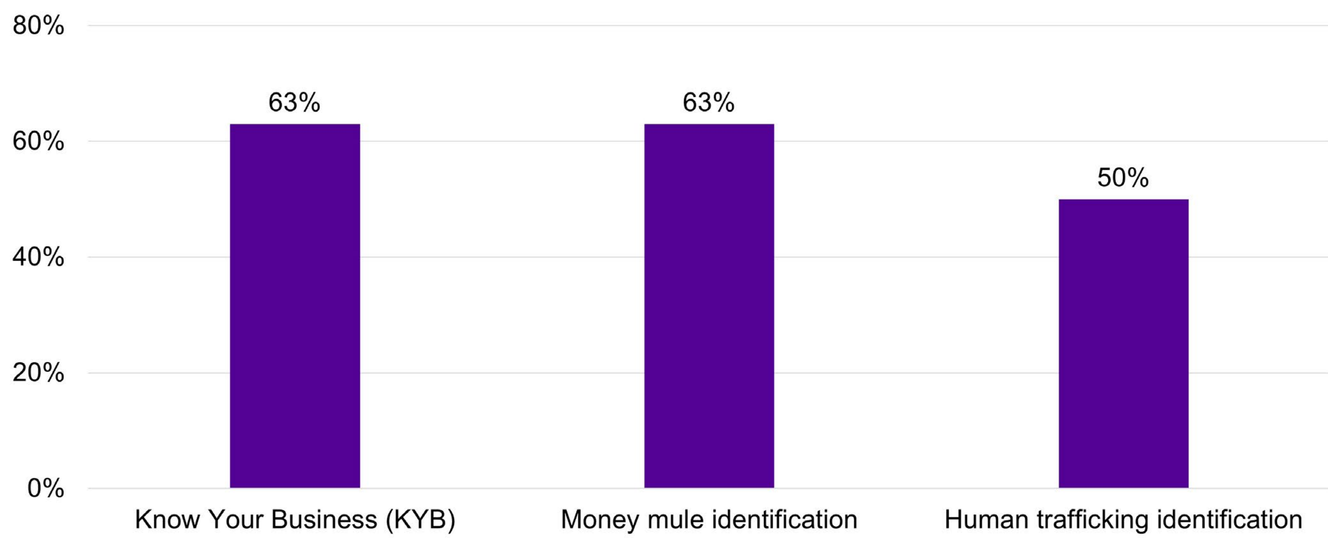
Use Cases: Meeting Every Objective

It's impossible for a KYC vendor to predict every necessity for every FI customer, which is why it's imperative that solutions be built to include as many possible use cases for all types of organizations across financial services. Javelin defines use cases within a KYC solution as those which fit explicit and specialized needs.

Because many of the criteria in this category are so heavily adopted across evaluated vendors, the differentiating offerings become crucial in elevating specific KYC vendors and solutions. The pervasiveness of money mule activity is often a topic of conversation between Javelin analysts and FIs, and the ability to detect and prevent such activity is a high priority for FIs. KYC vendors that offer this as a part of their existing product have an immediate advantage with FIs that are shopping around for KYC services. Moreover, other features like KYC for business (KYB: Know Your Business, or BKYC: Business Know Your Customer) and human trafficking identification may become key for FIs in identifying solutions that offer the widest range of use cases for their needs.

Uncommon Use Cases Criteria Become Essential in Identifying a Robust KYC Solution

Figure 4. Adoption of KYB, Human Trafficking, and Money Mule Identification



Source: Javelin Strategy & Research, 2023

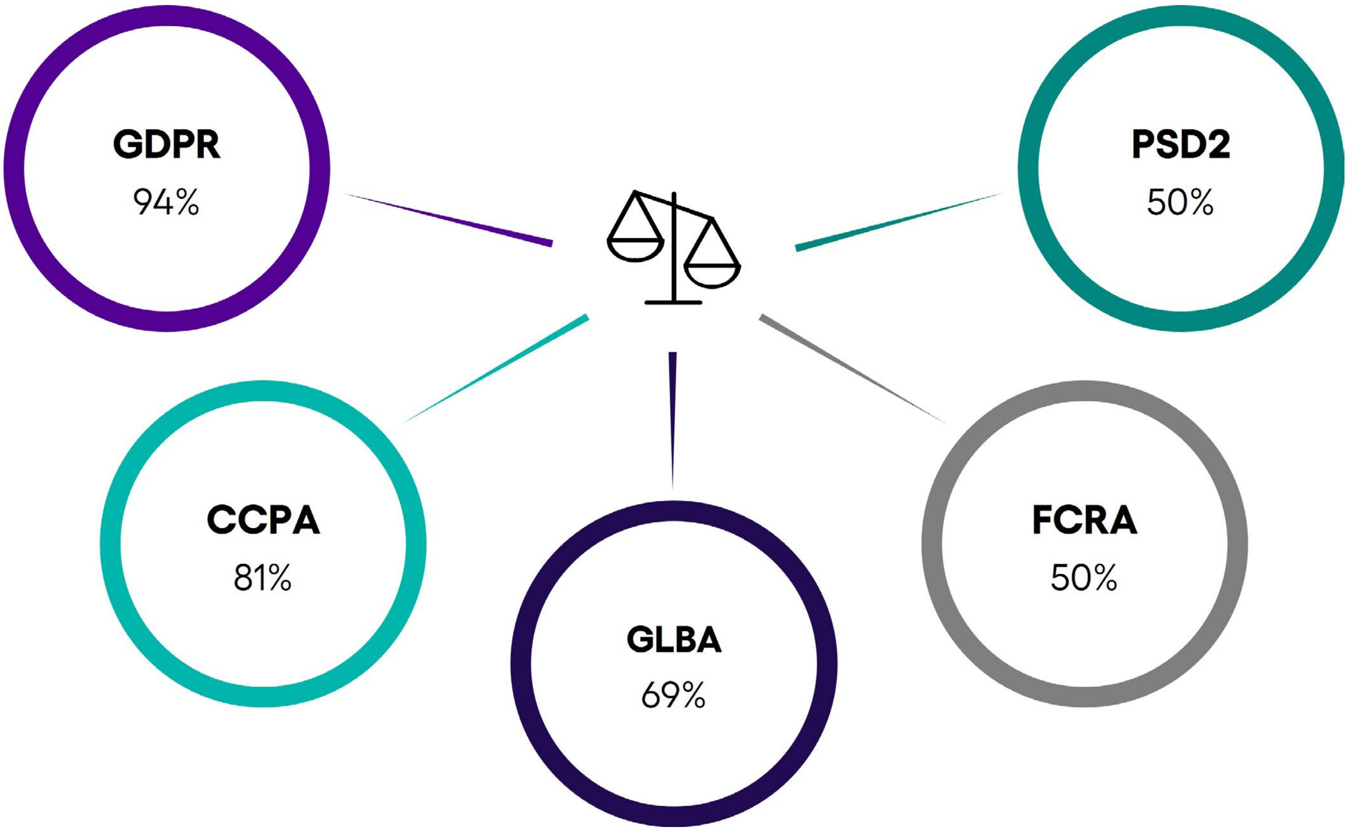
Although KYB/BKYC isn't necessarily a must-have, the prevalence of potentially fraudulent Economic Injury Disaster Loan and Paycheck Protection Program funds[6] makes KYB/BKYC something to consider adding to a solution's arsenal. The Office of the Inspector General estimates that the SBA improperly disbursed $200 billion in funds.

As previously mentioned, a superior KYC solution practices the responsible collection and use of consumer data to allow for the most accurate results in identity verification. This, in turn, allows FIs to make highly confident decisions in the account-opening process with existing and new customers and members. To maintain steady growth of new accounts, FIs must be able to foster a secure environment in which consumers feel safe sharing their PII.

Because the collection of PII and other relevant consumer data is critical to the KYC process—at account opening and for purposes of ongoing monitoring of account and transaction activity—data privacy, collection, and use regulations across the globe are highly regarded as important within the KYC sphere (see Figure 5).

Compliance with Regulation Designed to Protect Consumer Data is Key

Figure 5. Vendor Compliance With Various Regulatory Regimes



Source: Javelin Strategy & Research, 2023

The observance and adoption of ISO 20022 is quite low among evaluated vendors. Initial migration to the new common-language payments messaging standard began in March 2023, and current messaging won't be retired until 2025. Current adoption among ranked KYC vendors is at 31%; while this low percentage could be attributed to the deadline still being quite far into the future, the earlier organizations ready themselves for full adoption, the better they can anticipate and resolve issues.

An ISO 20022 Compliance Checklist[7] has been published to offer guidance on how to best be compliant with the new messaging standards, and for those vendors that have not yet begun the adoption process, it's time to start working on migration immediately. To take advantage of data-rich messaging for payments and better defend against identity fraud and financial crimes, vendors would be well-served to begin transitioning to the new standard sooner rather than later, allowing time for the inevitable migration issues to be resolved.

Use Cases Leaders

Use Cases	
1	Mitek
2	LexisNexis Risk Solutions
3	ComplyAdvantage

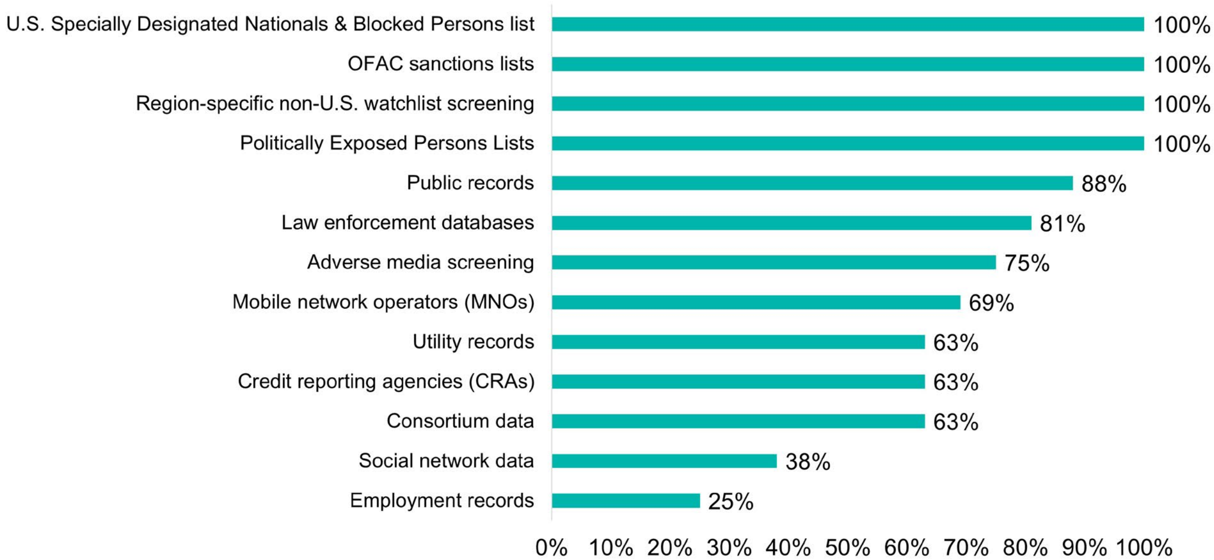
Mitek, LexisNexis, and ComplyAdvantage emerged as Leaders in the Use Cases category. All three providers are able to help financial institutions with identifying human trafficking—just half of vendors currently have a product designed to help FIs with human trafficking—and money mule identification (63%). Additionally, all three Leaders' solutions are being used to perform KYC for businesses, something only 63% of evaluated vendors can claim. Also taking a positive step toward payments messaging standards internationally, ComplyAdvantage and Mitek's solutions are compliant with ISO 20022, making them a part of the select few evaluated vendors that are ready for updated payments messaging before the November 2025 deadline.

Much like the criteria included in the Functionality category, the Use Cases category offers vendors plenty of opportunities to set themselves apart by offering features that aren't required for KYC compliance but enhance existing product offerings. FIs and other organizations in the business of verifying consumer identities will look for KYC vendors that are ahead of the pack in terms of anticipating regulatory updates, covering a wide range of potential business needs, like KYC as it relates to cryptocurrency exchanges or wealth management, or compliance with global consumer data protection guidelines. The goal is to ensure that FIs can maintain business as usual with steady account growth while providing the most robust protection against financial crimes of all degrees for internal systems and consumers. It's incumbent upon KYC vendors that wish to place themselves at the head of the pack to offer products that continue to meet KYC compliance requirements along with product enhancements that stay ahead of the trends in financial crimes and fraud.

Appendix

KYC Vendors Must Make Better Use of Oft-Forgotten Data Sources

Figure 6. Data Sources Accessed in Consumer Identity Verification Process



Source: Javelin Strategy & Research, 2023

Methodology

Data in this scorecard is based on requests for information (RFIs) conducted by Javelin Strategy & Research's Fraud & Security analysts with KYC solution providers. These RFIs were completed voluntarily by vendors from February 2023 to May 2023. Javelin reviewed only vendors that focus specifically on KYC-related tasks, honing our attention on 100 criteria in three categories:

1. Capabilities. A solution's ability to perform KYC-related tasks and use resources.
2. Functionality. A solution's user-facing controls, interface, and output customizations.
3. Use Cases. A solution's applicability to regulatory compliance initiatives and specific KYC-related missions.

Each category holds importance to the overall viability of a KYC solution, but Javelin analysts identified Capabilities as the most heavily weighted category, at 40% of the overall aggregate score, with many of the core purposes and tasks of the solution falling into this category. Following Capabilities in weighted importance is Functionality (35%), where organizations can tailor reporting outputs and controls to fit their specific business needs, creating a convenient and cost-effective resource. Use Cases closes out the KYC scorecard categories, weighing in at 25% of the overall score. This category holds a plethora of valuable criteria, allowing for organizations to fit a solution to meet specific KYC-related objectives.

Included in Javelin's evaluation are the following 16 KYC solution providers:

1. Alloy
2. AU10TIX
3. ComplyAdvantage
4. Equifax Identity & Fraud Services
5. Experian
6. FIS
7. GBG
8. Intellicheck Inc.
9. KYC-Chain
10. LexisNexis Risk Solutions
11. Mitek
12. Ondato
13. Plaid
14. SEON
15. Thales
16. Trulioo

Two additional KYC vendors completed RFIs but did not meet the minimum criteria adoption requirements for consideration (40% overall adoption):

- Passthrough
- Sila

Additional KYC Vendors were invited to participate in Javelin's evaluation but declined or did not respond.

Consumer data in this report was collected via an online survey conducted among 5,000 U.S. adults over the age of 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place from Nov. 7 through Nov. 21, 2022. Data is weighted using 18-plus U.S. population benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets. Due to rounding errors, the percentages on graphs may add up to 100% plus or minus 1%. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/- 1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the maximum margin of sampling error is +/- 3.22 percentage points at the 95% confidence level.

Additional consumer data in this report is based on information gathered from Javelin's Privacy Survey of 2,004 respondents in May 2022. Data was gathered and weighted to reflect a representative sample of the adult U.S. population. The margin of sampling error is ±0.94 percentage points at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.

Endnotes

1 Javelin Strategy & Research, "2023 Identity Fraud Study: The Butterfly Effect." Published March 28, 2023; accessed June 1, 2023.

2 Ibid.

3 ISO 20022, "ISO 20022 Frequently Asked Questions." Accessed June 15, 2023.

4 Financial Crimes Enforcement Network, "Bank Secrecy Act." Accessed June 30, 2023.

5 Financial Crimes Enforcement Network, "USA PATRIOT Act." Accessed June 30, 2023.

6 U.S. Small Business Administration, "COVID-19 Pandemic EIDL and PPP Loan Fraud Landscape." Published June 27, 2023

7 ISO 20022, "Compliance Checklist." Last updated June 12, 2023; accessed June 22, 2023.

Related Research

2023 Identity Fraud Study: The Butterfly Effect
March 2023
Over the 20 years Javelin Strategy & Research has been performing its landmark Identity Fraud Study, much has changed, including the emergence of an entire industry devoted to various methodologies for detecting, preventing, and reducing identity fraud. What hasn't changed is criminals' tenacity in seeking victims not just of traditional identity fraud but also identity fraud scams, which Javelin began tracking as a standalone category in 2020, providing a deeper, more granular view of identity fraud in the United States.

2022 Cyber-Trust in Banking Scorecard
September 2022
For consumers to trust their financial institutions, their expectations need to be met and exceeded. FIs must find the sweet spot at the junction of consumer privacy, cybersecurity empowerment, and cybersecurity education to maintain long-lasting relationships with their customers. This Javelin Strategy & Research scorecard ranks 21 of the largest financial institutions in the United States and outlines the steps needed to rise in the ranks and cultivate consumer trust.

2020 Identity Proofing Scorecard: Enterprise Solutions
November 2020
This report reviews and ranks technology providers that offer enterprise-wide identity-proofing solutions. Javelin evaluated 26 technology providers and created a ranking of the enterprise providers.

About Javelin

Javelin Strategy & Research, part of the Escalent family, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, lending, and wealth management. For more information, visit www.javelinstrategy.com.

Follow us on
Twitter and LinkedIn

javelin