Market Guide for KYC Platforms for Banking

10 December 2024 - ID G00811901 - 27 min read

By: Vatsal Sharma

Initiatives:Banking Industry Technology Insights

The shift toward digital KYC in banking is driven by changing regulatory requirements, operational factors and customer expectations. Bank CIOs should use this Market Guide to learn about the latest capabilities and vendor solutions that can help them with their evolving KYC needs.

Overview

Key Findings

- The market is split on “one-stop-shop” KYC platforms versus “best-of-breed” solutions. Approximately 47% of banking clients prefer consolidating their vendor relationships into a single, comprehensive KYC platform. Conversely, 38% of banks favor maintaining multiple vendor relationships to leverage specialized expertise in specific KYC areas.

- Artificial intelligence (AI)-enabled fraud, including deepfakes and synthetic identities, is on the rise, prompting vendors to prioritize investments in incorporating AI capabilities into their KYC solutions.

- The adoption of decentralized identity (DCI) solutions for bank KYC is in early stages, but market sentiment is positive about their potential. Sixty-six percent of respondents in Gartner’s vendor survey view DCI as having a transformational or significant impact by boosting efficiency, security, privacy and customer control over personal data.

- Perpetual KYC (pKYC) is rapidly gaining traction, driven by regulatory requirements, the need for real-time risk assessment and a comprehensive 360-degree customer view. pKYC involves continuous monitoring and updating of customer data, enabling banks to identify discrepancies between actual and expected customer behavior (as captured at onboarding), thereby mitigating potential threats and enhancing compliance.

Recommendations

- Assess your vendor strategy by considering your current KYC tech stack, operational needs and regulatory compliance requirements. For larger banks, maintaining multiple specialized vendors with strong orchestration capabilities is viable. Midtier, smaller banks and fintechs should consider consolidating to a single, comprehensive KYC platform that offers robust integration and configurability.

- Conduct stress tests on your current KYC processes using simulated AI attacks to assess resilience against evolving fraud tactics. Adopt a multipronged approach by augmenting liveness detection through a combination of techniques such as device fingerprinting, behavioral biometrics, geolocation and document scrutiny.

- Explore and pilot DCI solutions to stay ahead of the curve, focusing on vendors that offer compliance with KYC and AML regulations. Engaging with initiatives like the EU's digital wallet program, India's Aadhaar and similar projects around the world can offer insights for future integration of these solutions into your KYC processes.

- Collaborate with your analytics teams and compliance leaders to implement pKYC. An effective pKYC program unifies internal and external data into a single customer profile, automates updates, prioritizes material alerts and balances data collection with privacy regulatory compliance.

Market Definition

Gartner defines know-your-customer platforms as software solutions for banks to verify customer identity, conduct due diligence for assessing risk profiles and continuous monitoring to update customer info and risk status, and spot customer behavior deviations with an aim to ensure legal compliance.

Know-your-customer (KYC) platforms are indispensable tools for banks aiming to maintain regulatory compliance, minimize fraud and streamline the customer onboarding process. These platforms enable banks to perform the following critical tasks:

1. Customer identification program (CIP):

    - **Objective:** Identify and verify a customer's personal information during the onboarding process.

    - **Importance:** Ensures that the customer is who they claim to be, which is the first step in preventing fraudulent activities and complying with legal requirements.

2. Customer due diligence (CDD) and enhanced due diligence (EDD):

   - **Objective:** CDD involves assessing a customer's risk profile based on factors such as their occupation, source of income and country of residence, to name a few. EDD is applied to high-risk customers, requiring more thorough scrutiny, including sanctions and politically exposed person (PEP) screening.
   - **Importance:** Helps identify potential risks associated with customers and ensures that high-risk individuals undergo additional scrutiny to prevent money laundering and other illicit activities.

3. Continuous monitoring (CM):

   - **Objective:** Keep customer information current and accurate throughout the business relationship.
   - **Importance:** Involves regularly reviewing transactions, patterns and behaviors to detect and report unusual or suspicious activities, keeping an informed view of their risk status, thereby mitigating any fraudulent activities.

Business Objectives Addressed by KYC Platforms

Ability to Manage Risk

Compliance: KYC is a legal requirement in most jurisdictions and banks need to ensure adherence to various regulations like the USA Patriot Act, Financial Action Task Force (FATF) recommendations, Fourth and Fifth Anti-Money Laundering Directives (4AMLD and 5AMLD) (EU), Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) (Canada), Reserve Bank of India (RBI) KYC Guidelines and Financial Conduct Authority (FCA) Regulations (U.K.).

Consequences of noncompliance: Severe penalties, fines, legal repercussions and reputational loss can arise from failing to meet KYC requirements.

Ability to Minimize Fraud-Related Costs

Financial losses: Fraudulent activities can lead to direct financial losses, including unauthorized transactions and fraudulent withdrawals.

Liability: Banks are often responsible for reimbursing customers for these losses, which can impact their financial stability.

Ability to Improve Customer Experience and Enable Revenue Growth

Reputation management: Fraud and money laundering incidents can damage a bank's reputation, leading to a loss of customer trust.

Customer retention: A decline in customer base and reduced loyalty can result from perceived security weaknesses.

Market position: Negative word-of-mouth can affect the bank's market position and profitability.

Mandatory Features

- ID document assessment
- ID data extraction
- Third-party data connections to external sources to corroborate ID information
- Liveness detection and face comparison with ID document
- Sanctions, watchlist and PEP screening
- Transaction monitoring
- Case investigations
- Regulatory reporting
- Orchestration engine
- Workflow and case management

Common Features

- Alternative risk signals (e.g., device fingerprints, geolocation)
- Behavioral biometrics
- Prefilled customer application forms with verified identity information
- Adverse media coverage
- Qualified electronic signatures
- Portable digital identity or decentralized identity (DCI) wallet provision

- Single view of the customer
- Real-time risk scoring of customers
- Embedded client communication tools to streamline updates

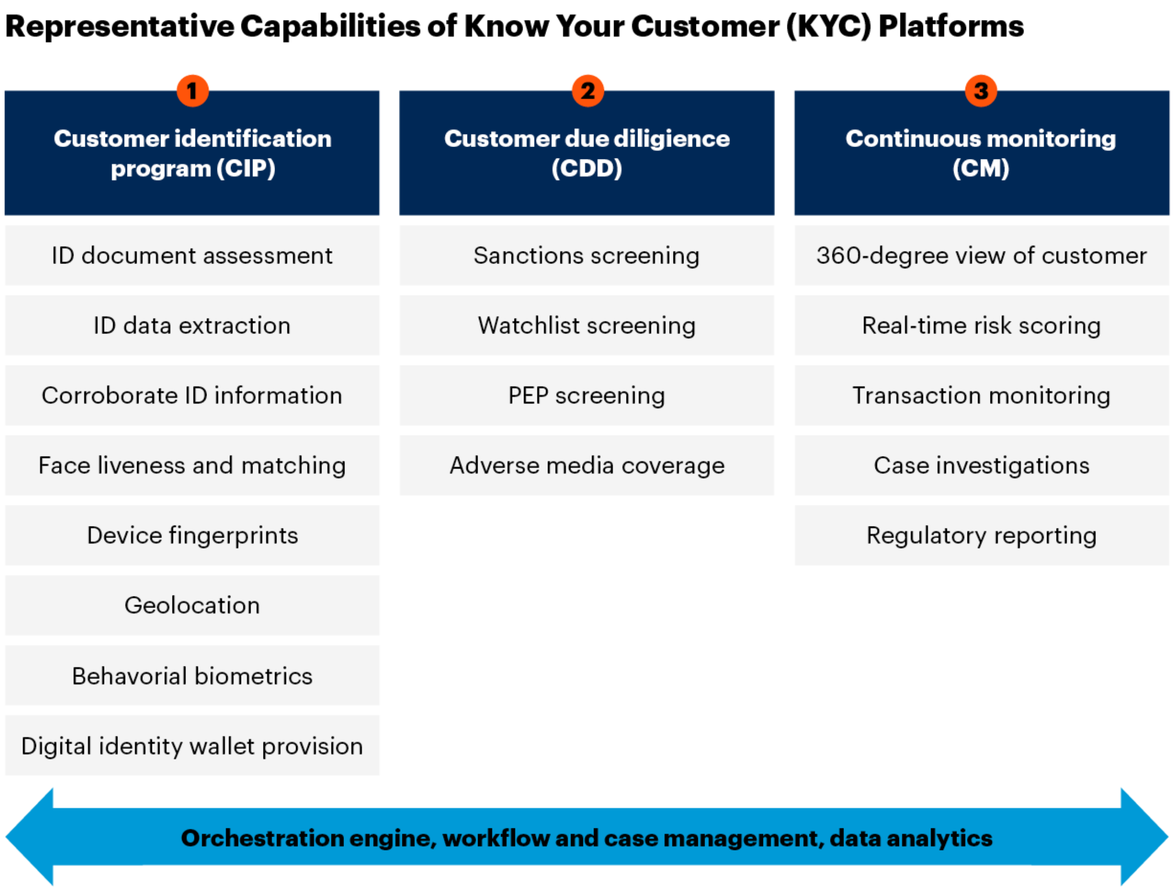
Market Description

The KYC solutions market is characterized by intense competition among a diverse array of players from global enterprises to regionally dominant firms. This competitive landscape is driven by the critical need for robust know your "X" capabilities — encompassing KYC, KYB (for businesses and vendors), and KYE (for employees) — across multiple industries, with the strongest interest from the banking sector due to stringent regulatory requirements. Each player brings unique strengths to the market. Larger vendors often highlight their ability to deliver comprehensive solutions across multiple geographies, streamlining KYC processes for global clients. Smaller firms try to differentiate based on deep understanding of local regulations, support for different ID documents and proprietary tech expertise for some key features (see Note 1).

Traditionally, vendors in this market started with specific core capabilities such as identity verification, sanctions screening, transaction monitoring, data provision/aggregation or risk scoring engines. Over time, they have expanded their offerings to provide end-to-end KYC solutions, achieved through a combination of in-house development, acquisitions and third-party partnerships. Consequently, most KYC platforms today are designed with modular features that offer flexibility and customization to meet the specific needs of banks. These platforms can integrate third-party capabilities to enhance overall functionality and effectiveness. For instance, access to third-party data allows for more comprehensive customer information, while alternative risk signals such as device fingerprinting, geolocation data and behavioral biometrics provide additional, nontraditional data points to better assess risk profiles. This integration is facilitated through an orchestration layer, ensuring connectivity and interoperability between the KYC platform and third-party services.

The KYC market growth is driven by increasing regulatory requirements and the need for enhanced risk management. This expansion is accelerated by the rising adoption of digital banking, the increasing sophistication of financial crimes, expectations of better customer experience and the demand for more efficient and effective KYC processes (see Figure 1).

Figure 1: Representative Capabilities of Know Your Customer (KYC) Platforms



Representative Capabilities of Know Your Customer (KYC) Platforms

1 Customer identification program (CIP)	2 Customer due diligence (CDD)	3 Continuous monitoring (CM)
ID document assessment	Sanctions screening	360-degree view of customer
ID data extraction	Watchlist screening	Real-time risk scoring
Corroborate ID information	PEP screening	Transaction monitoring
Face liveness and matching	Adverse media coverage	Case investigations
Device fingerprints		Regulatory reporting
Geolocation		
Behavorial biometrics		
Digital identity wallet provision		

Orchestration engine, workflow and case management, data analytics

Source: Gartner
811901_C

Market Direction

Move Toward Low-Effort Customer Experience and Faster Turnaround

Traditionally KYC has been approached primarily from a compliance and fraud management objective. However, bank priorities are evolving, and vendors are increasingly focusing on developing capabilities that help banks move toward a low-effort (yet diligent and compliant) customer experience.

A seamless and user-friendly interface ensures that customers can easily navigate through the KYC process without confusion or frustration. Vendors are looking to differentiate through intuitive user interfaces that provide clear instructions and minimize friction for end customers. For instance, vendors are incorporating step-by-step guides, real-time feedback and dynamic forms that adapt based on the information provided by the user. This reduces the likelihood of errors and incomplete submissions, thereby speeding up the onboarding process. Additionally, vendors are ensuring that the KYC process is equally smooth on mobile devices, catering to the increasing number of customers who prefer to open new accounts via their smartphones.

Automation is another critical area where vendors are making significant investments. By automating various aspects of the KYC process, vendors are reducing the need for manual intervention, which not only speeds up the process but also minimizes the risk of human error. For example, AI-enabled intelligent document processing tools assist in the extraction of data from a wide variety of document types — including handwritten and cropped documents — with varied levels of precision. Some of these tools are capable of data extraction even from partially visible or nondigitized text. The benefits include:

- Reduced manual intervention by automating the data extraction process
- Speeding up verification for faster processing times
- Minimizing errors with increased accuracy in data extraction

However, the challenge lies in handling the vast diversity of document formats and languages globally, necessitating continuous updates and training of AI models.

Additionally, GenAI agents are helping to streamline the CIP, CDD process and ongoing monitoring, enabling manual review teams with more accurate decision making and faster regulatory reporting. These agents can augment human investigators by helping with tasks such as automated search and data capture, review alerts, summarize findings, identify and prioritize material information and escalate cases as required. There are multiple vendors in the market offering such capabilities. For instance, SymphonyAI, WorkFusion, Lucinity, GreenLite, Ripjar and SilentEight. These AI-enabled automation capabilities allow banks to process a higher volume of KYC applications more efficiently, freeing up human resources to focus on complex tasks that require manual oversight.

Market Is Split on One-Stop-Shop KYC Platforms vs. Best-of-Breed Solutions

End-to-end orchestration capabilities have emerged as a pivotal feature in the KYC market, addressing the dual demands of banks seeking both consolidation and specialized expertise. According to the 2024 Gartner KYC vendor survey data, approximately 47% of banks are inclined toward consolidating their vendor relationships, favoring a single, comprehensive KYC platform that can streamline processes and enhance operational efficiency. Conversely, 38% of banks prefer maintaining multiple vendor relationships to leverage unique expertise in specific areas of KYC. [1] This dichotomy underscores the critical importance of orchestration capabilities, which enable integration and management of diverse KYC processes from data collection to verification and reporting. Vendors are offering dynamic configurability and API integrations, allowing banks to access all crucial data points and customize workflows to meet specific regulatory and operational requirements. While end-to-end orchestration capabilities can help bank CIOs achieve a holistic, efficient and compliant KYC process, regardless of their chosen vendor strategy, it's important to note that, in some cases, diverse systems that were not originally designed to work together may struggle to function cohesively.

Real-Time Risk Signal-Sharing Industry Networks Are Starting to Gain Momentum

The growing implementation of real-time risk signal-sharing networks, including banks and other industry participants (and potentially governments), is a timely move in the fight against organized crime. Criminals using advanced technologies and stolen data often stay a step ahead, increasing the velocity of their attacks and succeeding without detection. This evolving threat landscape necessitates agility from banks and a collaborative approach to enhance fraud detection capabilities right at the KYC stage during onboarding.

The development and implementation of cross-industry collaborative networks for sharing risk signals and real-time fraud detection are viewed as essential and expanding. According to the 2024 Gartner KYC vendor survey, 36% of respondents believe these networks will become indispensable, seeing widespread adoption across industries and government agencies, significantly bolstering real-time fraud detection. Another 32% foresee growing importance, with these networks improving fraud detection in key sectors such as banking that are prone to high fraud risks. [1] However, a quarter of industry participants feel these networks will only offer moderate improvements due to data privacy barriers and associated regulatory challenges. Some examples of such networks include:

- LexisNexis ThreatMetrix is a cross-industry risk intelligence network that shares real-time digital identity intelligence and fraud feedback with its participants.
- Experian's Hunter data network facilitates collective fraud detection by alerting participants in real time to suspicious information, matching it with other observed fraud events in the network.
- Jumio's 360-Degree Fraud Analytics analyzes potential fraud patterns across its cross-enterprise network as users go through ID verification during the KYC process.
- GBG Trust Network shares cross-sectoral identity intelligence, analyzing potentially suspicious anomalies and high-velocity submissions in real time. The network assigns a trust score to identity data, reflecting potential fraud risk without sharing actual personally identifiable information (PII).
- Identiq's network operates across various industries, including fintechs, travel, e-commerce, ticketing, marketplaces and telcos. It validates user identities against each participating organization's databases through anonymized queries and responses to preserve privacy.

Market Analysis

Perpetual KYC Is Becoming Increasingly Important

Continuous or perpetual KYC (pKYC) is rapidly gaining traction in the industry, driven by the imperative to maintain real-time risk assessment and achieve a comprehensive 360-degree view of the end customer. Unlike traditional periodic reviews, which often result in outdated information and delayed risk detection, pKYC ensures that customer data is continuously updated and monitored. This dynamic approach allows banks to detect and respond to risks as they emerge, thereby enhancing compliance and mitigating potential threats before they escalate (see KYC and AML Challenges and Opportunities for Banking CIOs).

Real-time risk assessment is a cornerstone of pKYC, enabling banks to evaluate suspicious customer behavior instantaneously. Vendors are leveraging advanced algorithms and data analytics to assess risk factors in real-time, providing actionable insights that help banks make informed decisions quickly. This proactive approach not only enhances regulatory compliance; it also reduces the likelihood of financial crimes such as money laundering and fraud. For instance, continuous monitoring of transactions and behavioral patterns can flag anomalies that may indicate fraudulent activities, allowing banks to take immediate corrective actions.

In addition to real-time risk assessment, a 360-degree view of the end customer is essential for effective pKYC. This feature integrates data from diverse sources, including transaction histories, social media and public records into a unified profile. A holistic view of the customer aids better decision making, improves customer relationship management and offers opportunities for more robust compliance.

Moreover, the integration of pKYC into the banking ecosystem offers significant operational efficiencies. By automating data updates and risk assessments, banks can reduce the manual workload on compliance teams, thereby lowering operational costs and minimizing human errors. This continuous updating mechanism ensures that the customer data is always current, reducing the risk of compliance failures due to outdated information.

While the advantages of pKYC are substantial, its implementation presents certain challenges. Banks that traditionally rely on one-time KYC, supplemented by periodic manual reviews, may face significant upfront investments in tech solutions and personnel training to transition to a pKYC model. Additionally, if not carefully managed, pKYC can generate unnecessary alerts, overwhelming compliance teams and obscuring actual risks. To address this, it is crucial that bank CIOs choose vendor solutions that are capable of highlighting materially new information about customers and filter out irrelevant data. Furthermore, continuous data collection must be balanced with stringent compliance to privacy regulations to ensure both regulatory adherence and customer trust.

Vendors Are Investing in AI to Improve Document Assessment and Liveness Detection Capabilities

Recent advances and easy access to highly sophisticated AI-based tools have enabled fraudsters to up their game. Bad actors are using these tools to create synthetic identities and conduct deepfake attacks that have the potential to bypass traditional identity verification systems. The 2024 Gartner KYC vendor survey data shows that most vendors are prioritizing the integration of AI capabilities into their KYC solutions, identifying this as their top focus for the next two years. [1]

Document assessment and data extraction is a key area where vendors are investing in AI. This includes developing machine learning (ML) models and fraud detection algorithms to enhance document verification capabilities. The techniques are utilized for various tasks, including:

- **Document recognition:** Identifying and classifying different types of documents

- **Assessing security features:** Verifying the presence and authenticity of security features in documents
- **Tackling document forgery:** Identifying inconsistencies that may indicate tampering

Some vendors claim to have developed models capable of identifying specific artifacts left behind by the GenAI tools used by criminals, adding an extra layer of security against sophisticated fraud tactics. However, optical- or visual-based assessments have limitations due to the increased sophistication in counterfeit development. As an additional security measure, some vendors offer near-field communication (NFC)-based authentication, which can be considered more deterministic and reliable for chip-based documents. The user experience can be challenging because not all identification documents are equipped with chips, something common in most passports. Specifically, driving licenses in the U.S. and U.K. typically lack this feature, requiring users to rely on their passports for verification. This necessity can complicate the process, as users may find it less convenient to access their passports compared to more readily available forms of ID like driver licenses or state IDs.

Vendors are increasingly leveraging AI to enhance biometric verification and liveness detection capabilities for eKYC. Liveness detection is a key step in the identity verification process. This involves customers taking a selfie or recording a short video of their face, which is used to assess the genuine presence of an individual. Active liveness detection involves prompting users to perform specific actions, such as blinking or smiling, which AI algorithms analyze in real time to assess if the moving images are that of a live person. Passive liveness detection, on the other hand, uses AI to analyze subtle cues like skin texture and lighting reflections without requiring user actions.

Fraudsters utilize various tactics to breach banks’ identity verification measures. Presentation attacks, where they use printed photos or digital screens, are countered with techniques that identify inconsistencies in texture, depth and light reflection. Injection attacks involve directly inserting a deepfake image or video into the vendor’s API or software development toolkits (SDKs), bypassing the user’s device camera entirely. While presentation attacks are relatively easy to execute, injection attacks require more technical expertise, making them harder to carry out but also more challenging to detect.

Deepfake detection tools employ AI models to identify synthetic media by detecting anomalies and artifacts indicative of deepfake generation. For instance, some vendors are using background (discrepancies in lighting, shadows or other details that do not align naturally with the foreground subject) and feature (such as facial landmarks, skin texture and microexpressions) analysis to detect deepfakes and identify high-risk clusters (see Emerging Tech: The Impact of AI and Deepfakes on Identity Verification).

Matching user selfie to ID involves algorithms comparing a selfie taken by the user with the photo on their government-issued ID, analyzing facial features and skin texture to ensure a match. In 1:1 matching, AI models perform a one-to-one comparison between a selfie and a single reference image to confirm identity. Some vendors may also perform 1:N matching in which the selfie or face image from the document is compared with previous IDV checks to look for repeated faces possibly associated with different identities. This can be a powerful way to detect fraud, but means that consent must be given to the IDV vendor to store PII data from previous IDV checks.

Nonetheless, the effectiveness of these models depends heavily on the quality and volume of training data. There is also the risk of adversaries using AI to create more sophisticated attacks, necessitating a continuous arms race between fraudsters and vendor solutions.

Assessing Vendor Capabilities

Vendors sometimes use similar marketing language and metrics to highlight their capabilities, making it challenging for bank CIOs to distinguish between claims. Bank CIOs can take some practical steps to validate vendor assertions:

1. **Certifications:** Ensuring that the vendor’s solutions are certified by reputable agencies. For example:

   - National Institute of Standards and Technology (NIST) conducts the Face Recognition Vendor Test (FRVT) to evaluate the accuracy and performance of facial recognition systems, including their ability to detect spoofing attempts (liveness detection) across various demographics.

   - FIDO Alliance offers a “Face Verification Certification” program that assesses liveness detection and bias in facial recognition technologies.

2. **Compliance with international standards:** ISO/IEC 30107-3 is an international standard for biometric presentation attack detection (PAD), which outlines the methods and criteria for evaluating the effectiveness of biometric systems in detecting fraudulent attempts.

3. **Client references and case studies:** Speaking with existing clients and reviewing case studies can provide insights into the real-world impact of the vendor's technology and verify that the solutions have delivered measurable benefits.

4. **Back testing:** Testing the vendor's solutions against your own data (through POCs) to evaluate pass-through and fraud detection rates.

By taking these steps, CIOs can better assess the true capabilities, ensuring they select the most effective and reliable technologies for their needs.

Decentralized Identity Has the Potential to Upend/Disrupt the Current KYC Model

Decentralized identity (DCI), a type of portable digital identity (PDI), is emerging as a pivotal innovation in the evolution of bank KYC process. The importance of DCI is underscored by its ability to offer a verifiable and reusable identity that customers can use in bank account opening, as well as across multiple platforms and services.

These solutions address two critical issues in traditional KYC processes:

1. **They enhance security by reducing the risk of identity fraud and data breaches.** By leveraging decentralized technologies, it ensures that personal data is stored securely in the form of verifiable credentials (VCs) that are cryptographically secured in a digital identity wallet (DIW) (likely installed on a smartphone) and only shared with authorized parties. This is particularly important in an era where data privacy regulations are becoming increasingly stringent.

2. **DCI solutions improve customers' control over their personal data.** Customers can manage their identity information and consent to data sharing, thereby enhancing trust and transparency. They can opt for minimal data sharing, such as confirming they are over 18 years old without disclosing their actual birthdate.

Moreover, the adoption of DCI solutions can lead to significant operational efficiencies for banks. By providing a single, verifiable identity, these solutions streamline the onboarding process, reducing the need for repetitive identity checks and manual interventions. This not only speeds up the KYC process but also reduces operational costs.

Apple and Google Wallet in the U.S. and Alipay in Asia/Pacific are allowing some residents to store their driver's licenses and state IDs digitally on their mobile devices. It's important to note that while these wallets are also a type of PDI, they lack the security and privacy features of DCI. They store digital representations of government-issued IDs rather than verifiable credentials. Additionally, several countries have implemented some form of digital ID system that partially helps with bank KYC, for example, Estonia (e-Identity), Sweden (BankID), Norway (e-ID), India (Aadhar and Digilocker), Hong Kong (iAmSmart), Dubai (UAE Pass), South Korea (K-DID) and Singapore (Singpass).

The market is starting to explore a new and different way of approaching identity data for banking customers. The push from the European Commission (via eIDAS 2.0 regulation) that will require all EU member states to make a DIW available to citizens by 2026 is a key step in this direction. There are four large-scale consortiums — POTENTIAL, EWC, DC4EU and NOBID — that are testing EU DIWs before their roll-out to member states. One of the key use cases for DIW is bank account opening. We are seeing a number of proofs-of-concept (POCs) and some production use cases, but it is still early, and this technology has not yet reached a threshold of widespread adoption. European banks are watching closely and engaging with the EU's digital wallet program and its implications for KYC and client onboarding. While the EU is asking member states to issue digital wallets through dedicated apps, banks and other private players may also be asked or allowed to issue wallets.

By 2026, at least 500 million smartphone users will be regularly making verifiable claims using a digital identity wallet built on distributed ledger technology (see Market Guide for Decentralized Identity).

Several vendors are offering products that enable banks to benefit from DCI for the KYC use case. There is positive sentiment in the market about the potential of DCI solutions. According to the 2024 Gartner KYC vendor survey data, 32% of respondents perceive these solutions as transformational, fundamentally changing KYC processes by enhancing security, privacy and customer control over personal data. Another 34% believe that these solutions will play a significant role in improving and streamlining KYC processes, contributing to better compliance and customer experience. [1]

However, despite these positive developments, challenges related to the adoption of DCI for KYC remain. For DCI solutions to be viable in the financial services industry, they must comply with KYC and anti-money-laundering (AML) regulations. While several vendors claim to have the functionality within their DCI solutions to comply with these regulations, banks often find it difficult to make a compelling business case for transitioning away from their traditional compliance processes, despite their inherent challenges. One frequently cited challenge is developing a monetization model for digital wallets. Among the key parties involved — issuers (for verified credentials and digital wallets), wallet holders (customers) and verifiers/relying parties — determining a monetization model based on benefit realization, privacy and security remains unresolved. There are multiple proposals under deliberation but no final approach has been agreed upon in the industry.

Due to these challenges, one-third of respondents see a moderate to limited impact of DIW and feel that these solutions will not gain significant traction within the banking sector. [1]

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Selection

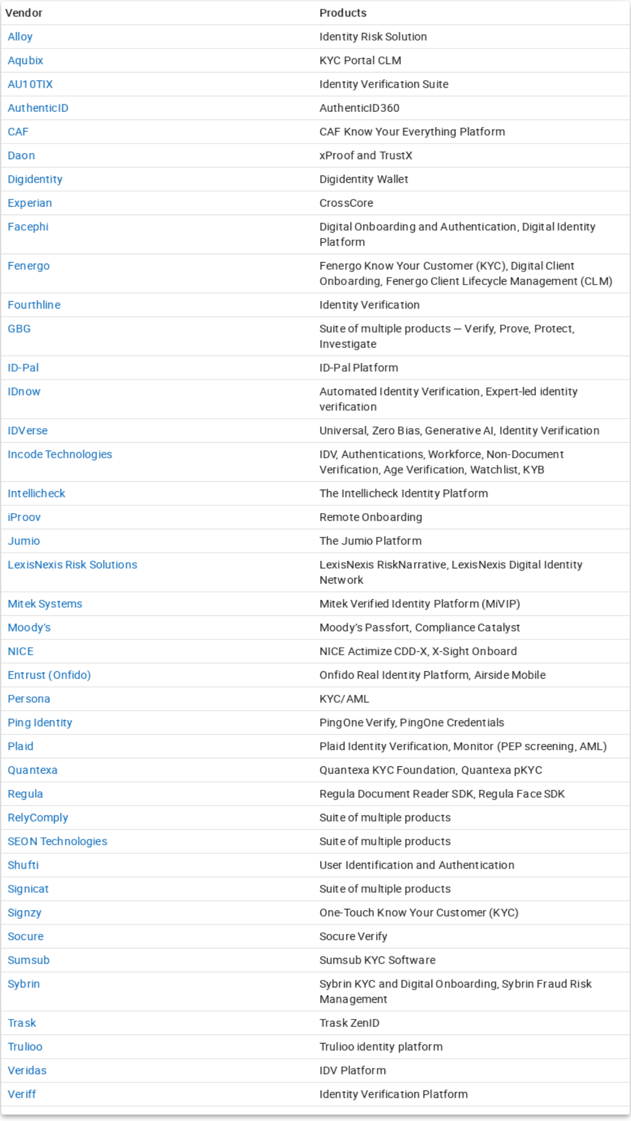
The listed vendors in this research represent what's core in the KYC solutions market, what extends it and what will transform it. They were selected based on one or more of the following criteria:

- Vendors providing end-to-end KYC capabilities across CIP, CDD and CM, either through proprietary solutions or third-party partnerships.
- Vendors focused on banking as one of their key market segments.
- Vendors offering capabilities that are unique, innovative and/or demonstrate forward-looking product strategies.
- Frequent inquiries by Gartner clients about a particular vendor for KYC use cases.
- Vendors that represent particular market segments or geographic regions, thus helping to illustrate the breadth of the market.

The representative vendors here do not constitute an exhaustive list of all providers with these characteristics; we are limited by Gartner methodology to a maximum number of vendors that can be listed in this research note. Necessarily, many worthy vendors have been omitted with no implied criticism; neither is inclusion an endorsement.

Table 1: Representative vendors in KYC

(Enlarged table in Appendix)



Vendor	Products
Alloy	Identity Risk Solution
Aqubix	KYC Portal CLM
AU10TIX	Identity Verification Suite
AuthenticID	AuthenticID360
CAF	CAF Know Your Everything Platform
Daon	xProof and TrustX
Digidentity	Digidentity Wallet
Experian	CrossCore
Facephi	Digital Onboarding and Authentication, Digital Identity Platform
Fenergo	Fenergo Know Your Customer (KYC), Digital Client Onboarding, Fenergo Client Lifecycle Management (CLM)
Fourthline	Identity Verification
GBG	Suite of multiple products — Verify, Prove, Protect, Investigate
ID-Pal	ID-Pal Platform
IDnow	Automated Identity Verification, Expert-led identity verification
IDVerse	Universal, Zero Bias, Generative AI, Identity Verification
Incode Technologies	IDV, Authentications, Workforce, Non-Document Verification, Age Verification, Watchlist, KYB
Intellicheck	The Intellicheck Identity Platform
iProov	Remote Onboarding
Jumio	The Jumio Platform
LexisNexis Risk Solutions	LexisNexis RiskNarrative, LexisNexis Digital Identity Network
Mitek Systems	Mitek Verified Identity Platform (MiVIP)
Moody's	Moody's Passfort, Compliance Catalyst
NICE	NICE Actimize CDD-X, X-Sight Onboard
Entrust (Onfido)	Onfido Real Identity Platform, Airside Mobile
Persona	KYC/AML
Ping Identity	PingOne Verify, PingOne Credentials
Plaid	Plaid Identity Verification, Monitor (PEP screening, AML)
Quantexa	Quantexa KYC Foundation, Quantexa pKYC
Regula	Regula Document Reader SDK, Regula Face SDK
RelyComply	Suite of multiple products
SEON Technologies	Suite of multiple products
Shufti	User Identification and Authentication
Signicat	Suite of multiple products
Signzy	One-Touch Know Your Customer (KYC)
Socure	Socure Verify
Sumsub	Sumsub KYC Software
Sybrin	Sybrin KYC and Digital Onboarding, Sybrin Fraud Risk Management
Trask	Trask ZenID
Trulioo	Trulioo identity platform
Veridas	IDV Platform
Veriff	Identity Verification Platform

Source: Gartner (December 2024)

Market Recommendations

- Tailor your KYC vendor strategy to your unique organizational needs:
  - Larger banks (Tier 1 and Tier 2) often have the resources to manage multiple vendor relationships and may benefit from specialized expertise in different aspects of KYC. Bank CIOs leading such institutions should focus on vendors that offer robust orchestration capabilities to integrate these multiple systems.
  - Midtier, smaller banks, credit unions and fintechs typically prefer consolidation to reduce IT burden and vendor management complexity. A single, comprehensive KYC platform with strong orchestration capabilities would be more suitable.
  - Bank CIOs looking to mitigate risks associated with relying on a single provider should consider maintaining multiple vendor relationships. While some banks aim to transition to a single, centralized platform, they often encounter challenges in displacing existing KYC tech stacks. Consequently, continuing to work with multiple vendors, even if perceived as a less optimal strategy, can provide greater resilience and flexibility in their KYC processes.
- Assess the robustness of your current KYC processes against AI-enabled attacks:
  - Retail bank CIOs should partner with risk and compliance teams to conduct stress tests on your current KYC processes through simulated AI attacks. The aim of this exercise is to see if the current processes can withstand new-age attacks and fraud tactics.
  - A multipronged approach to deepfake detection in KYC processes enhances security by combining multiple techniques and data sources. By integrating device fingerprints, behavioral biometrics, geolocation, document scrutiny, and both active and passive liveness detection, organizations can create a robust defense against deepfakes and injection attacks.
  - Retail bank CIOs should verify vendor claims through client references, back-testing the vendor's solutions against your own data to evaluate pass-through and fraud detection rates and relying on international standards (ISO/IEC 30107-3) and industry certifications such as NIST and FIDO for benchmarking vendor claims.

- Embrace pKYC for real-time risk assessment and enhanced compliance:
  - Retail bank CIOs should work closely with risk and compliance leaders to implement/strengthen effective pKYC. Ensure that customer data is continuously updated and monitored, allowing for timely detection and response to emerging risks, thereby enhancing compliance and mitigating potential threats before they escalate. Conduct continuous monitoring of transactions and behavioral patterns to flag anomalies, reducing the likelihood of money laundering and fraud.
  - Adopt vendor solutions that help integrate data from internal and external sources into a unified profile to provide a holistic view of the customer, improving decision making and customer relationship management. Automate data updates to reduce the manual workload on compliance teams, lowering operational costs and minimizing human errors. To avoid overwhelming compliance teams with unnecessary alerts, CIOs should select vendor solutions that highlight materially new information and filter out irrelevant data.
  - Finally, balance continuous data collection with stringent compliance to privacy regulations to ensure both regulatory adherence and customer trust.

- Plan for integrating digital identity wallets into your KYC process:
  - CIOs should actively explore and pilot DCI solutions to stay ahead of the curve. Start engaging vendors offering DCI solutions to gain a better understanding of their capabilities, security measures and compliance features. This will enable you to assess your readiness and select the most suitable solutions that align with your specific KYC requirements and regulatory standards.
  - Join/monitor initiatives like the EU's digital wallet program to gain firsthand experience and insights into the implementation and benefits of digital identity wallets. Participating in these pilot programs will allow you to test/understand the feasibility and effectiveness of DCI solutions in a controlled environment before full-scale deployment.
  - Keeping abreast of these developments will help CIOs make informed decisions, adopt best practices and stay ahead of industry trends, ensuring your bank remains competitive and compliant.

Evidence

[1] **2024 Gartner Financial Services Know Your Customer Vendor Survey.** The main objective of this survey was to understand vendor offerings and perspectives of know your customer (KYC) solutions. This survey was conducted online from 17 July through 1 October 2024. In total, 50 vendor organizations responded. *Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

KYC and AML Challenges and Opportunities for Banking CIOs

Quick Answer: How Will Digital Wallets Evolve in the Future?

Hype Cycle for Financial Crime, 2024

Magic Quadrant for Identity Verification

Market Guide for Decentralized Identity

Case Study: Deep Fraud and Financial Crime Detection Built With Generative Adversarial Networks

Table 1: Representative vendors in KYC

Vendor	Products
Alloy	Identity Risk Solution
Aqubix	KYC Portal CLM
AU10TIX	Identity Verification Suite
AuthenticID	AuthenticID360
CAF	CAF Know Your Everything Platform
Daon	xProof and TrustX
Digidentity	Digidentity Wallet
Experian	CrossCore
Facephi	Digital Onboarding and Authentication, Digital Identity Platform
Fenergo	Fenergo Know Your Customer (KYC), Digital Client Onboarding, Fenergo Client Lifecycle Management (CLM)
Fourthline	Identity Verification
GBG	Suite of multiple products — Verify, Prove, Protect, Investigate
ID-Pal	ID-Pal Platform
IDnow	Automated Identity Verification, Expert-led identity verification
IDVerse	Universal, Zero Bias, Generative AI, Identity Verification

Incode Technologies	IDV, Authentications, Workforce, Non-Document Verification, Age Verification, Watchlist, KYB
Intellicheck	The Intellicheck Identity Platform
iProov	Remote Onboarding
Jumio	The Jumio Platform
LexisNexis Risk Solutions	LexisNexis RiskNarrative, LexisNexis Digital Identity Network
Mitek Systems	Mitek Verified Identity Platform (MiVIP)
Moody’s	Moody’s Passfort, Compliance Catalyst
NICE	NICE Actimize CDD-X, X-Sight Onboard
Entrust (Onfido)	Onfido Real Identity Platform, Airside Mobile
Persona	KYC/AML
Ping Identity	PingOne Verify, PingOne Credentials
Plaid	Plaid Identity Verification, Monitor (PEP screening, AML)
Quantexa	Quantexa KYC Foundation, Quantexa pKYC
Regula	Regula Document Reader SDK, Regula Face SDK
RelyComply	Suite of multiple products
SEON Technologies	Suite of multiple products
Shufti	User Identification and Authentication

Signicat	Suite of multiple products
Signzy	One-Touch Know Your Customer (KYC)
Socure	Socure Verify
Sumsub	Sumsub KYC Software
Sybrin	Sybrin KYC and Digital Onboarding, Sybrin Fraud Risk Management
Trask	Trask ZenID
Trulioo	Trulioo identity platform
Veridas	IDV Platform
Veriff	Identity Verification Platform

Source: Gartner (December 2024)