IDC MarketScape

IDC MarketScape: Worldwide Identity Verification in Financial Services 2025 Vendor Assessment

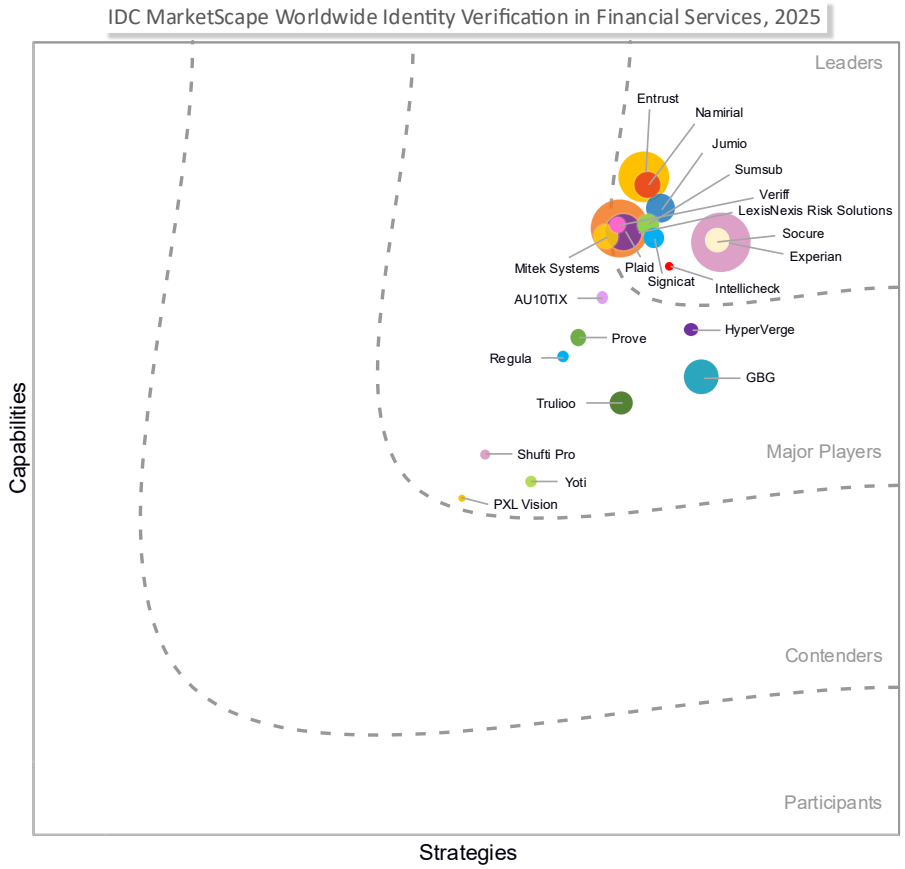
Sam Abadir

THIS EXCERPT FEATURES EXPERIAN AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Identity Verification in Financial Services Vendor Assessment



Source: IDC, 2025

September 2025, IDC #US52985325e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Identity Verification in Financial Services 2025 Vendor Assessment (Doc # US52985325).

IDC OPINION

Strategic Shifts in Financial Services Identity Verification

New Dynamics Shaping Identity Verification

Adoption of identity verification (IDV) in financial services has accelerated dramatically, coinciding with shifts in user expectations, fraud risk, and technological opportunity. What is striking today is not only the volume of digital identity checks being performed but also the transformed nature of how these checks are designed, delivered, and governed.

A particularly noteworthy dynamic is the swift integration of generative AI (GenAI) within IDV workflows. The expansion of GenAI across financial institutions has made advanced document analysis, behavioral modeling, and anomaly detection not just more efficient but more user centric. GenAI-driven tools are being used to auto-populate onboarding forms, interpret a wide spectrum of global documents, and even translate user interfaces or adapt to new fraud patterns in real time. What once required substantial engineering is now accessible through intuitive interfaces and automated back-end orchestration. This democratization of AI, where frontline business or compliance teams can leverage advanced identity signals without deep technical training, has driven a new class of adaptive, "smart" verification journeys.

Not only are solutions more intelligent, but the level of ease with which they can be implemented and flexibly adapted has improved. What was previously a drawn-out process of customization is now facilitated by low-code configuration, AI-backed recommendations, and modular plug-ins. This shift is expanding the practical use of IDV to smaller financial institutions, new market entrants, and teams that would not have previously had the resources to deploy robust verification frameworks.

As IDV moves from the realm of pure fraud defense into a driver of digital trust and commercial agility, institutions are also challenging vendors to balance sophistication with simplicity. The competitive field is rewarding those platforms that can keep the underlying technical muscle invisible while delivering intuitive, guided user and

customer service experiences. The result is a new expectation of speed, usability, and universal accessibility in IDV implementation and operations.

Use Case Innovation: Expanding the Boundaries

Beneath the surface of compliance checklists, financial services organizations are confronting a proliferation of new and evolving identity verification use cases. As Table 1 illustrates, the range now spans foundational functions such as new account opening and transaction monitoring through highly specialized requirements like EU Digital Identity (EUDI) Wallet adoption and regulatory reporting. Together, these represent a heterogenous but increasingly mature landscape, shaped by regulatory mandates, fraud pressures, and shifting customer expectations.

IDV is no longer confined to verifying identities at onboarding. Instant lending, digital investment onboarding, and remote employee or vendor verification require dynamic, context-aware assurance. Cross-border commerce and multi-jurisdiction customers add complexity where ID formats, local laws, and compliance rules diverge. Synthetic identity detection, high-risk merchant onboarding, and high-risk product enrollment stretch the role of IDV into active fraud defense and long-term risk management.

Crucially, this diversity of use cases demonstrates that balancing friction and growth is now a strategic imperative, not just an operational detail. While the industry often seeks frictionless experiences to drive adoption, the right level of friction, such as additional verification at high-risk moments, is essential for deterring fraud, satisfying regulatory scrutiny, and reinforcing long-term trust. Institutions must calibrate IDV flows to context, recognizing that a well-placed checkpoint can be preferable to risking unchecked access or exposure.

European-driven initiatives such as national eIDs, eIDAS 2.0, and the EUDI Wallet show how IDV is also becoming embedded in legal trust frameworks and digital identity ecosystems, shaping the next phase of compliance and customer experience. Meanwhile, behavioral biometrics and continuous signals are expanding the boundaries of what constitutes valid proof of identity, moving from static checks to ongoing assurance. In a landscape as diverse as the one outlined in Table 1, success will depend on using IDV not only to verify identity but to strategically balance growth, compliance, and trust.

TABLE 1

Identity Verification Use Case Framework for Financial Services

IDV Use Case	Definition	Business Drivers	Key Challenges	Success Measures
New account opening	Verifying customer identity at onboarding for banking, payments, or wealth	Compliance with AMLD5/AMLD6, KYC, fraud prevention, and customer experience	Thin-file applicants, document diversity, and false rejects	Approval speed, abandonment rate, and fraud loss reduction
Risky/high-value transaction	Extra verification for flagged or large transactions	AML compliance, PSD2 SCA, and fraud detection	Latency in real-time detection and friction	Fraud detection percentage and real-time response
Age verification	Confirming legal age for services (e.g., crypto, trading platforms)	Compliance with national laws and reputational risk	Fake IDs and minors bypassing	Percentage success and reduction in fines
Remote employee/ third-party onboarding	Validating identities of staff, contractors, or vendors	Insider risk reduction and third-party oversight	Limited data sets and fragmented systems	Reduced insider fraud and onboarding time
Account recovery/ password reset	Identity reverification during recovery	Prevent ATO and maintain trust	Balancing friction versus fraud risk	Reduced ATO and faster recovery
Cross-border/ multi-jurisdiction customer	Verification across EU and global contexts	PSD2, AMLD6, FATF, and consistency in CX	ID format diversity and rules complexity	Coverage breadth and fraud reduction by region
Synthetic identity/fraud prevention	Detecting and stopping synthetic identities	Prevent mule accounts, credit fraud, and AML risk	Evolving fraud tactics and lack of shared intel	Reduced synthetic ID fraud
eIDAS 2.0 compliance and trust services	Using identity verification aligned with EU eIDAS trust framework	Legal enforceability, regulatory compliance across EU, and PSD2/AML integration	Cost and complexity of QES issuance and interoperability	Audit acceptance, cross-border enforceability, and number of QES issued
EUDI Wallet adoption and interoperability	Supporting the EU Digital Identity Wallet for reusable credentials	Compliance with regulation 2024/1183, cross-border onboarding, and customer control of identity	Wallet adoption, ecosystem maturity, and varying member state readiness	Wallet usage rates, re-KYC cost reduction, and interoperability success

TABLE 1

Identity Verification Use Case Framework for Financial Services

IDV Use Case	Definition	Business Drivers	Key Challenges	Success Measures
European national eIDs integration	Leveraging SPID, ID Austria, ITSME, German eID, and others for IDV	National eID compliance, PSD2 SCA, and local regulatory mandates	Fragmentation across national schemes and UX trade-offs	eID coverage, onboarding time, and customer adoption
Customer due diligence (CDD/EDD)	Risk-based verification under AMLD6	AMLD6 compliance and sanctions avoidance	Data quality and scaling monitoring	False positives reduction and audit pass
High-risk merchant/ business onboarding (KYB)	Verification of merchants/UBOs	AMLD6, FATF recommendations, and fraud prevention	Ownership complexity and missing data	Onboarding time and fraud reduction
Ongoing authentication/ continuous assurance	Ensuring identity assurance beyond onboarding	Reduce ATO and PSD2 compliance	Privacy rules (GDPR) and consent	Continuous fraud reduction and login success
High-risk product/service enrollment	Verifying applicants for credit, lending, crypto, and gambling	AMLD6, national regulations, and fraud prevention	Fraud targeting and UX	Loan default rates and fraud prevented
Regulatory reporting and audit	Leveraging IDV records for compliance audits	PSD2, AMLD6, and GDPR evidence	Maintaining evidentiary quality	Audit pass rate and reduced manual effort

Source: IDC, 2025

Core Capabilities: Insights and Observations

The industry's capabilities matrix remains crowded and highly standardized at the feature level; genuine differentiation demands looking beyond simple feature sheets. Table 2 illustrates the contemporary framework for evaluating identity verification solutions, organizing key capabilities and strategic imperatives now recognized across leading financial institutions. Further:

- User trust and regulatory acceptance are now as dependent on transparency and auditable processes as on technical efficacy. The ability to demonstrate

explainability and governance over automated or AI-driven verification is quickly becoming a central competitive challenge.

- Integration depth matters. Organizations are measuring vendors not only by external checks and verification accuracy but also by how fluidly identity signals flow into operational systems for customer service, transaction monitoring, and long-term relationship management.
- The platforms winning the confidence of major institutions are those that balance rigorous control with operational agility. This means supporting institution-led change with limited vendor dependency and empowering nonengineering/data science teams to react quickly as regulations, threats, and business models evolve.
- Balancing friction and growth is now a strategic imperative, not just an operational detail. While the market often seeks "frictionless" experiences to drive adoption, the right level of friction, such as additional verification at high-risk moments, can be essential for deterring fraud, satisfying regulatory scrutiny, and reinforcing long-term trust. Institutions must calibrate IDV flows to context, recognizing that a well-placed checkpoint can be preferable to risking unchecked access or exposure.

TABLE 2

Core Capabilities of Identity Verification Platforms in Financial Services

Capability	Definition
Identity establishment and verification	
Documentation	
Data collection	The user provides personally identifiable information (PII) (e.g., name, date of birth, address).
	The system may collect additional metadata, such as IP address and device fingerprinting, to assess risk.
Document verification	The user submits a government-issued ID (e.g., passport, driver's license, national ID card).
	Advanced tools use optical character recognition (OCR) to extract text and AI-driven document forensics to detect tampering.

TABLE 2

Core Capabilities of Identity Verification Platforms in Financial Services

Capability	Definition
Identity snapshot	
Biometric verification	In selfie matching, the user takes a live selfie to compare against the ID photo using facial recognition.
	In liveness detection, AI ensures the user is present and not using a static image or deepfake.
Decision support	
External data	
Database and third-party checks	The system cross-checks user data against global watch lists, credit bureaus, and government databases.
Risk assessment and ongoing compliance	
Risk assessment and decisioning	AI models score the risk of fraud or identity theft.
	Manual review teams may intervene for flagged cases.
	Based on confidence levels, the system approves, rejects, or requests further verification.
	Synthetic identity identification is included.
Workflow orchestration	The ability to configure, branch, and adapt verification flows is based on rules, risk signals, and user context without heavy coding. It supports conditional step triggering and fallback routing.
Rules and policy configuration	Flexible, no-code/low-code tools define risk thresholds, data validation logic, document acceptance rules, and fraud detection triggers.
Ongoing compliance and authentication	
Monitoring	
Ongoing monitoring and authentication	Some IDV tools provide continuous authentication via behavioral biometrics. Reverification may be required for high-risk transactions or regulatory compliance.

TABLE 2

Core Capabilities of Identity Verification Platforms in Financial Services

Capability	Definition
Compliance	
Data privacy and consent management	The IDV platform captures and stores user consent records, enforces data minimization, and ensures regional data sovereignty compliance (e.g., GDPR, LGPD).
Operational enablement	
Integration	
Integration and API connectivity	It involves seamless connections with CRM, onboarding platforms, case management tools, and core banking systems and includes prebuilt connectors for third-party data and compliance providers.
Reporting	
Analytics and reporting	There are dashboards, drill-down metrics, and exportable reports for operational performance, pass/fail rates, step-level drop-off, and fraud patterns.
User experience	
User experience and accessibility	It involves mobile-first capture optimization, multi-language interfaces, accessibility compliance (WCAG), and support for low-bandwidth/offline environments.

Source: IDC, 2025

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To ensure relevance and comparability, inclusion in this IDC MarketScape was limited to identity verification vendors that demonstrate both functional breadth and proven traction within financial services. Vendors had to meet the following criteria:

- **Functional capabilities:**
  - Support data collection of personally identifiable information (PII) and metadata
  - Provide document verification
  - Offer biometric verification, including selfie matching with liveness detection

    - Enable database and third-party validation
    - Deliver risk assessment and decisioning capabilities
    - Include ongoing monitoring and authentication features
- **Market presence:**
    - Multiple referenceable financial services clients across banks, credit unions, insurance (excluding health), and wealth management
    - At least some deployments in production for one year or longer, demonstrating sustainability and operational maturity

These requirements ensure that evaluated vendors are both technically capable and established within the financial services industry, with proven ability to meet regulatory, fraud prevention, and customer onboarding needs.

ADVICE FOR TECHNOLOGY BUYERS

Selecting the right identity verification platform in financial services is an important decision that reaches beyond technical specifications. Buyers should look for solutions that align with strategic needs, regulatory expectations, and practical workflows, ensuring both operational flexibility and long-term resilience.

When evaluating platforms, adaptability to real-world scenarios is a primary consideration. Financial institutions increasingly operate across diverse channels, including web-based and app-based self-service, call center, and face-to-face verification. Solutions should either provide built-in workflow capabilities or support seamless integration with external workflow engines to ensure configurability of verification processes. The ability to tailor workflows enables institutions to manage both remote digital onboarding and in-person customer verification while maintaining consistency and compliance across different contexts. Further:

- Identity verification systems should enable institutions to create and adjust verification steps across multiple scenarios, facilitating adoption across digital, in-person, and hybrid channels.
- Platforms should provide either native workflow functionality or robust integration capabilities, allowing institutions to leverage existing enterprise tools or manage verification directly within the identity verification platform.

Regulatory demands now shape not only which identities require verification but how that verification is conducted. Institutions should prioritize systems that provide granular control over verification steps, whether through integrated workflow or embedded decisioning logic. Additional checks should be triggerable based on risk signals, transaction value, geographic location, product type, or interaction channel. Escalation paths must be configurable, with automated handling for routine cases and

manual reviews available for flagged activity. This flexibility supports both efficient routine processing and thorough investigation when exceptions or risks are identified. Further:

- Flexible configuration allows IDV platforms to apply the right level of scrutiny according to specific business and risk criteria.
- Automated and manual escalations help institutions balance speed with thoroughness, responding quickly to risk without disrupting everyday operations.

Ongoing compliance is only as strong as an institution's ability to monitor, report, and respond to regulatory needs. Buyers should demand platforms with robust audit support, such as dashboards for real-time visibility, historical event logs, exportable compliance data/reports, and access to specialized customer service resources for audit and documentation requests. This ensures institutions can confidently maintain oversight and respond to regulatory audits and internal reviews. Further:

- Real-time and historical reporting tools support daily oversight and formal audit preparation.
- Easily accessible audit trails and responsive support channels streamline documentation and regulatory engagement.

The practical realities of implementing or replacing an IDV solution also matter. Institutions benefit from piloting new tools and processes with limited groups before scaling, which helps identify issues and confirm compliance before wider rollout. When transitioning from legacy platforms, data migration must be secure and compliant, with enterprisewide access to previously collected user consent records preserved, if applicable, to ensure ongoing regulatory obligations are met. Analytics features allow institutions to continuously monitor conversion rates, fraud incidents, compliance interventions, and operational performance, ensuring ongoing optimization. Further:

- Pilot testing workflows in controlled groups, followed by measured scaling, reduces operational risk and supports regulatory assurance.
- Analytics and reporting capabilities enable ongoing process improvement and rapid response to emerging risks or business needs.

Finally, platforms should support dynamic friction management, enabling institutions to calibrate verification rigor based on risk level and context. This approach keeps onboarding smooth for low-risk activities but introduces extra checks when warranted, supporting both commercial agility and security. Transparency with customers about verification procedures and data protection builds trust and supports compliance. Further:

- Configurable friction points mean institutions can deliver efficient service without sacrificing fraud prevention.
- Transparent communication about verification enhances customer confidence and trust in digital interactions.

By prioritizing these capabilities, financial institutions can select IDV platforms that offer the flexibility, oversight, and workflow adaptability necessary to meet present requirements and future changes. Careful selection and ongoing refinement will ensure investments deliver both regulatory assurance and superior customer experiences.

The considerations outlined previously demonstrate that selecting an identity verification platform extends well beyond technical evaluation. These decisions directly shape compliance readiness, fraud prevention, operational efficiency, and customer experience. Because of this, risk, compliance, technology, operations, and customer-facing teams all need to be part of the evaluation process. The advice to the buyer is to evaluate solutions through the lens of each of these roles, confirming that platforms provide the workflow configurability/integration, audit transparency, and dynamic risk management each group requires. IDV should be assessed not only for its technical features but for its ability to serve as a shared capability that enables alignment across functions and supports both regulatory assurance and customer trust. Table 3 maps the primary themes of this analysis to the organizational roles most directly impacted.

TABLE 3

Impact of Identity Verification Across the Financial Services Organization

Capability Theme	Primary Impacted Roles	Key Responsibilities
Workflow adaptability across channels	CIO/CTO, COO, product managers, and branch operations managers	Ensure workflows function in digital, call center, and branch environments; align with customer experience goals.
Integration or built-in orchestration	Enterprise architects, IT integration leads, and CIO	Decide whether to leverage native workflow tools or connect to external engines; maintain interoperability with existing systems.
Risk-based checks and escalation paths	CRO, CCO, AML officer, and fraud prevention manager	Configure workflows to trigger additional verification based on risk signals; manage manual reviews of flagged cases.
Audit, monitoring, and reporting	CCO, internal audit, DPO, and regulatory liaison	Maintain real-time oversight, audit trails, and compliance reporting; respond to regulator and board inquiries.
Implementation and optimization	IT security manager, analytics and reporting lead, and digital product owners	Oversee pilot testing, secure data migration, and continuous monitoring of fraud, compliance, and performance metrics.
Dynamic friction and customer trust	COO, customer service leads, and KYC operations teams	Balance verification rigor with seamless onboarding; ensure transparent communication with customers.

Source: IDC, 2025

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Experian

Experian is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide identity verification in financial services.

Experian is headquartered in Dublin, Ireland, with major operational centers in Costa Mesa, California, and offices in 32 countries. Established in its current form in 1980,

with historical roots dating to 1826, Experian provides identity verification and fraud prevention services integrated into its broader data and analytics offerings. Its identity verification platform incorporates access to consumer credit files, proprietary data assets, and configurable orchestration capabilities for regulated industries.

Experian's platform integrates with core banking systems, payment processors, and legacy and cloud-native architectures through real-time APIs. These APIs support customizable risk scoring models, multichannel authentication flows, and progressive onboarding logic. Experian also supports fraud orchestration through behavioral analytics, device intelligence, and transaction-level risk scoring.

The company applies generative AI across its fraud prevention stack. Applications include automating parts of the modeling life cycle, conducting real-time threat detection, and refining decision automation. Experian has incorporated bot and behavioral analytics technology through its acquisition of NeuroID, enhancing its ability to identify anomalous digital behavior and coordinated attacks.

Experian's orchestration infrastructure enables step-up authentication flows triggered by behavioral anomalies, device risk, or transaction thresholds. These flows can include additional verification layers such as biometric validation or document reverification. The company's behavioral analytics framework does not require the collection of additional personally identifiable information to detect anomalies.

Support infrastructure includes 24 x 7 technical support, global professional services, and compliance consulting. Experian maintains an ecosystem of financial institutions, technology providers, and fintechs across North America, Europe, and Asia/Pacific. Its offerings align with jurisdiction-specific KYC and AML obligations, including GDPR and other privacy frameworks.

Strengths

- Access to a broad and diverse range of proprietary identity and credit data sources enables multilayered verification across different financial services use cases.
- The platform incorporates risk-based authentication, progressive onboarding, and behavioral analytics that enable fraud detection with reduced friction.
- NeuroID integration expands capabilities in behavioral monitoring, including detection of fraud rings and bot behavior during digital onboarding.

Challenges

- The scale of personal data used in identity verification processes may elevate regulatory scrutiny under global privacy laws such as GDPR.

- Coverage gaps for thin-file, underbanked, and unbanked populations require supplementary verification sources. Effective orchestration and adoption of orchestration capabilities are critical to realizing value.

Consider Experian When

Experian is ideally considered by regulated financial institutions and high-volume digital platforms seeking data-rich, compliance-aligned verification workflows, with integration options for both legacy systems and cloud-native environments.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

As a result, this IDC MarketScape provides both a snapshot of which vendors are most capable today and a forward-looking view of which vendors are best positioned to meet the evolving needs of financial institutions in the next three to five years.

This IDC MarketScape is intended to guide financial institutions in aligning vendor selection with their specific requirements. Vendor placement should be interpreted as directional rather than prescriptive. Every vendor evaluated in this document offers viable identity verification products, and every financial institution brings unique regulatory, operational, and customer experience requirements. As such, the IDC MarketScape does not account for every scenario or buyer priority. Institutions should

use this analysis to inform a short list and then conduct deeper evaluations that reflect their own strategic and operational context.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

The worldwide financial services identity verification (IDV) market comprises technologies and services that establish, authenticate, and continuously monitor customer and business identities across digital and physical channels. Core capabilities include data collection, document verification, biometric authentication, database and third-party checks, risk assessment and decisioning, workflow orchestration, rules and policy configuration, ongoing monitoring and authentication, data privacy and consent management, integration and API connectivity, analytics and reporting, and user experience and accessibility (refer back to Table 1). These solutions support regulatory compliance, fraud prevention, and customer trust by enabling secure onboarding, transaction verification, and life-cycle identity management. The market spans comprehensive platforms as well as specialized tools that integrate through APIs and orchestration layers. Demand is driven by regulatory mandates, rising fraud threats, and the need for frictionless digital experiences across banking, payments, and insurance.

LEARN MORE

Related Research

- *Redefining Trust: The Case for Smarter Identity Verification in Banking* (IDC #US53564225, June 2025)
- *Customer Identity: The Foundation for AI-Infused Retail Banking Growth* (IDC #US52948725, March 2025)

- *The Rise of Agentic AI and Agentic Workflow in KYC — Emerging Vendors Redefining Process Management for IT Buyers* (IDC #US52910825, February 2025)
- *Bank Regulation in 2025 and Beyond* (IDC #lcUS53191425, February 2025)
- *FinCEN Publishes Alert on Deepfakes and the Future of Fraud: A Call to Action for Identity Verification Innovators* (IDC #lcUS52735924, November 2024)

Synopsis

The IDC study evaluates leading providers of identity verification (IDV) solutions used across banking, payments, insurance, and wealth management. It highlights how IDV has evolved from a compliance checkbox into a core enabler of digital trust, fraud prevention, and customer experience. Market trends such as generative AI, orchestration platforms, behavioral biometrics, and dynamic risk management are reshaping both vendor strategies and institutional expectations.

The document underscores that while baseline capabilities such as document verification, biometric checks, and third-party validation have become table stakes, differentiation now lies in workflow flexibility, integration depth, transparency, and adaptability to regulatory and fraud pressures. Institutions must balance efficiency with trust by selecting vendors that can scale across multiple channels, adapt to evolving risk signals, and maintain clear auditability. This IDC MarketScape provides financial institutions with a structured view of vendor capabilities and strategies, enabling buyers to align technology selection with long-term resilience and customer trust objectives.

"The next generation of identity verification is defined by adaptability," says Sam Abadir, research director, IDC Financial Insights for Risk, Financial Crime, and Compliance. "Financial institutions need solutions that scale across channels, calibrate rigor to risk, and provide full transparency while enabling them to choose the right customer experiences at the right moment to balance compliance, growth, and trust."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com