The Future of Identity Verification:

5 Threats and 5 Opportunities

Regula

Table of Contents

Identity verification is no longer a back-office function. In 2025, it sits at the center of how digital economies run: shaping customer trust, regulatory compliance, and business resilience. Every login, transaction, and customer interaction is now a trust decision, and the stakes are rising fast.

The challenge is that most organizations are caught between two realities. On one side: legacy systems, fragmented tools, and KPIs designed to measure losses after the fact. On the other: new threats moving at enormous speed, regulators demanding accountability, and customers expecting seamless trust as the default. The gap between the two has never been wider.

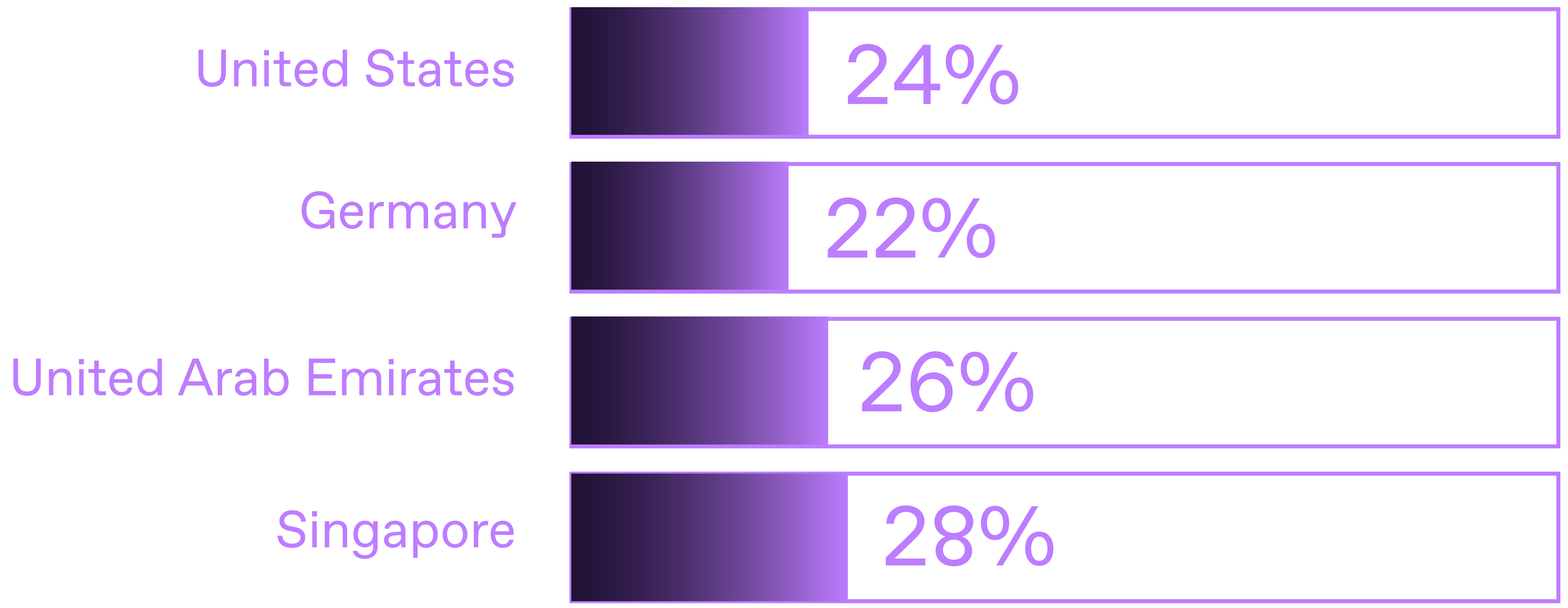
This report outlines the industry's efforts to address this challenge and deal with rising fraud. The path leads toward biometric-first verification, orchestration instead of fragmentation, budgets that reflect board-level urgency, and responsibilities that shift from manual firefighting to proactive defenses. Identity verification is evolving from a tactical safeguard to the backbone of digital business. The pages ahead trace that transition, as well as the contradictions, risks, and opportunities shaping it.

Methodology

Regula partnered with Censuswide to survey

567

decision-makers in fraud detection, prevention, and financial crime across four global markets:



The research took place between 2025-03-28 – 2025-07-09.

Participants represented industries with high exposure to identity fraud and digital risk: Aviation (15%), Banking (28%), Crypto (13%), Fintech (16%), Healthcare (12%), and Telecommunications (15%).

All research was conducted in line with the Market Research Society (MRS) Code of Conduct and ESOMAR standards. Censuswide is a member of both the MRS and the British Polling Council.

In 2 Minutes: The 10 Things You Need to Know

This report highlights 10 critical shifts—five threats and five opportunities—that show how identity verification in 2025 is caught between two forces: industrialized fraud and the urgent race to reinvent defenses.

Threats: Where the Ground is Cracking

1 Deepfakes Hit Prime Time

No longer niche: one in three firms is already battling AI-driven impersonation at scale.

2 Your Tools Are Outdated

MFA and basic biometrics still dominate, but they alone are no match for more advanced identity threats.

3 Still Measuring Yesterday's Losses

Chargebacks and fraud costs remain the top KPIs, leaving prevention out of sight.

4 The Automation Trust Gap

Everyone wants automation, but few are ready to bet on it fully.

5 Fraud Training on Paper Only

Awareness programs are mainly tick box exercises, with only a few firms teaching how to identify and protect against real AI-powered attacks.

Opportunities: Where the Future Is Being Built

1 Biometrics As the Default

Face scans and liveness checks are fast becoming the new frontline of trust.

2 Orchestration: The Hidden Superpower

Fragmented stacks are today's weak point—unified orchestration is tomorrow's edge.

3 Budgets Go Into Overdrive

Executives are done with incrementalism—exponential growth is the new normal.

4 Responsibilities Get Rewired

Fraud teams are done with paperwork and firefighting—the future is policies, ML, and forensics.

5 From ID Checks to Trust Infrastructure

Identity verification is graduating from a tactical step to the backbone of digital business.

Key Numbers

For organizations with significant fraud exposure ($1M+ losses),

deepfakes hit 4 out of 10 companies

For highly affected organizations with losses exceeding $5M,

deepfakes and synthetic IDs top the list as the most common fraud types

Biometric verification rises to the #1 choice

in the ideal future tools setup, overtaking multi-factor authentication and behavioral biometrics

Chargeback rate 18%

and cost of fraud 17%

are the top KPIs tracked. Both are reactive, not preventive

66% of firms

have passed the halfway mark on automation

79%

say they should ideally be there in the future

Employee training ranks #4

in responsibilities today, yet almost no firms train against AI-powered attacks

Over half of executives would love to see

fraud prevention budgets grow more than 20%

in the next cycle

Over 1 in 4

firms want IDV fully integrated

across all business functions—not just fraud and compliance

> Fraud isn't about fake passports anymore. The front line has shifted to verification itself. Deepfakes, synthetic IDs, and AI-driven impersonation are hammering the very step we once trusted most. For companies buried under thousands of fraud cases a year, this is already the nightmare happening in real time.
>
> What stands out in the data is the disconnect. Everyone says automation is the answer, but most firms stay stuck in the middle, half-automated and half-exposed. Teams track chargebacks instead of prevention. They run awareness training but never drill against real AI threats. That gap between what we know and what we do is exactly where attackers move in.
>
> The way forward isn't mysterious: automate what machines do best, orchestrate the tools into one flow, and let humans focus on the calls that really matter. Identity verification has to graduate from a box-checking step to the backbone of trust. The companies that get there first won't just stop fraud—they'll own the future of digital business.

Ihar Kliashchou,
Chief Technology Officer at Regula

Threats: Where the Ground Is Cracking

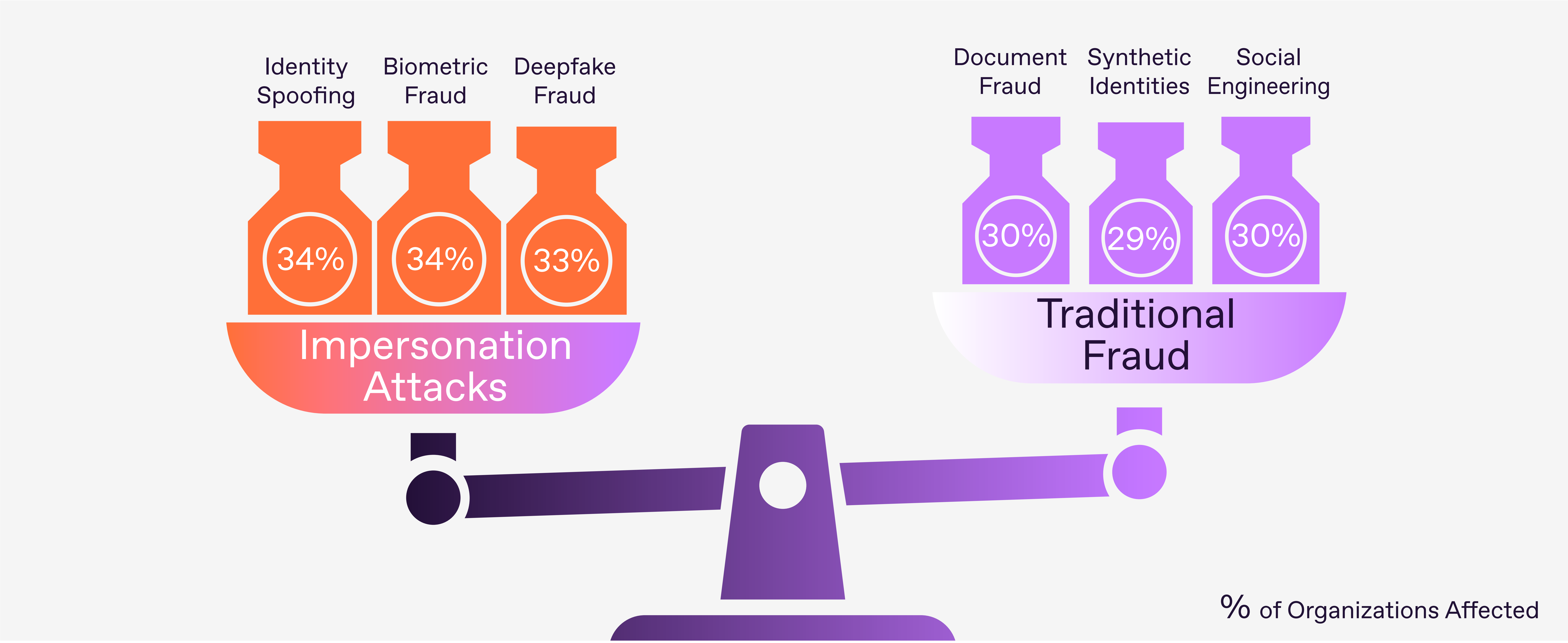
1 Deepfakes Go Mainstream: Fraud at Scale

Graph 1. Top 3 Most Frequent Fraud Types, globally

Fraud Type	Identity Spoofing	Biometric Fraud	Deepfake Fraud
% of Organizations Affected	34%	34%	33%
What's Faked & How	Simple props: printed photos, screen images, or replayed selfies/videos.	Fake fingerprints, silicone masks, or 3D face models to bypass biometric sensors.	AI-generated faces, voices, or videos that mimic or invent identities.
Key Trait	Cheap and basic: works when checks are weak.	Physical attack on biometrics: needs materials and effort.	Scalable, adaptive, and hard to spot.
Common Scenarios	Used to open bank or fintech accounts in bulk with stolen photos, giving fraudsters fake accounts for scams or money mule networks.	Used for SIM swaps or account resets so criminals can take over real users' accounts and steal funds.	Used in video ID checks at banks/crypto platforms, creating fake customers at scale. After passing KYC checks, fraudsters can get "clean" accounts to move or hide money.

Identity fraud has never been static, but our survey reveals a dramatic rebalancing of tactics in the past year. For decades, counterfeit documents and stolen credentials defined the fraud landscape. Today, these traditional methods are still present, but they no longer dominate. Instead, the battlefield has moved toward impersonation: the deliberate manipulation of identity signals—biometric, video, and synthetic—that target both human verifiers and machine algorithms.

Graph 2. The New Balance: Impersonation Attacks vs Traditional Fraud



What unites these techniques is their shared goal: convincing a system that the fraudster is someone else, whether by replaying a stolen face, creating a synthetic persona, or morphing voices and videos in real time. The age of manufactured identities has arrived.

Fraudsters aren't waiting until after onboarding anymore. The new favorite target is the verification step itself. By slipping in at the entry point, attackers gain clean access to accounts and services under false identities, staying invisible to fraud checks that only kick in later.

Document fraud still appears in smaller organizations, but the pattern is shifting at scale. High-loss and high-volume firms are facing industrialized, AI-driven impersonation.

The data shows minimal variation between industries, as fraudsters leverage nearly identical attack vectors (biometric fraud, spoofing, document fraud), with biometric fraud appearing in 5 of 6 industries and only slight ranking differences based on each sector's specific vulnerabilities.

For organizations with significant fraud exposure ($1M+ losses),

deepfakes hit

4 out of 10

companies

For highly affected **organizations with losses exceeding $5M,**

deepfakes and synthetic IDs top the list as the most common fraud types

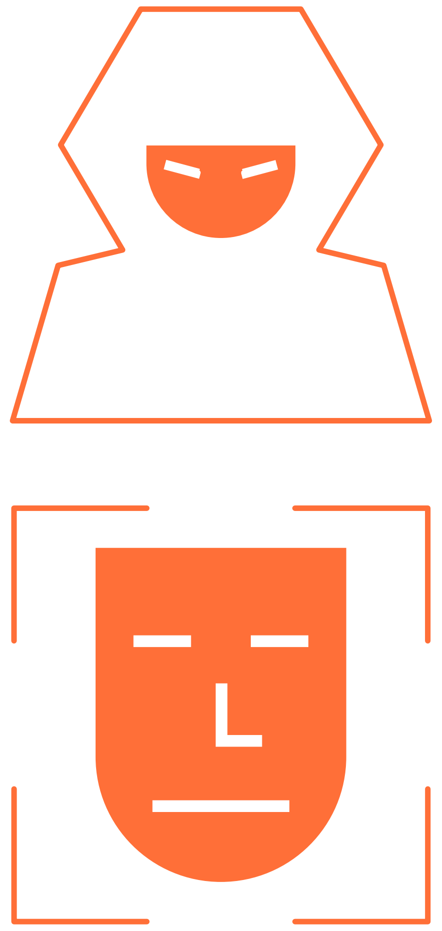


Table 1. Top 3 Fraud Types by Sector

Industry	#1	#2	#3
Aviation	Deepfake	Social engineering	Biometric fraud
Banking	Biometric fraud	Identity spoofing	Deepfake
Crypto	Biometric fraud	Document fraud	Social engineering & synthetic ID fraud
Fintech	Identity spoofing	Deepfake	Document fraud
Healthcare	Document fraud	Social engineering	Biometric fraud
Telecoms	Biometric fraud	Identity spoofing	Synthetic ID fraud

Case volumes reveal how fraud evolves as it scales. At the low end (<26 cases in 2024), organizations mostly battle document fraud (37%)—opportunistic scams relying on forged papers. In the moderate range (26–250 cases), the threat mix shifts to biometric fraud (39%), with social engineering (33%) emerging as a significant risk. Once volumes exceeded 251 cases in 2024, fraud became industrialized: identity spoofing (40%) and deepfakes (38%) dominated. This trajectory shows that what begins as one-off opportunistic attacks quickly evolves into systematic, AI-driven impersonation at scale once fraudsters find enough volume to automate.

Three forces drive this shift. First, the post-pandemic boom in remote onboarding removed physical checks, creating a digital-first attack surface. Second, AI tools have become cheap, fast, and repeatable: fraudsters can now mass-produce convincing synthetic identities. Third, many firms built strong document verification but underinvested in biometric liveness detection, leaving a wide gap for attackers.

i Deepfakes are no longer fringe threats—they are the main driver of identity fraud at scale. For firms exposed to high-volume, high-loss deepfake attacks presentation attack detection (PAD) and advanced liveness have become baseline requirements, not optional add-ons.

2 The Tools Don’t Match the Threats

Table 2. Current vs. Ideal Toolsets – Top 5

Rank	Currently Used	Ideal Setup	What It Signals
1	Multi-factor authentication	Biometric verification	Strong demand for trusted, user-friendly security
2	Behavioral biometrics	Human expert review	Required in some geographies for compliance-sensitive scenarios
3	Biometric verification	Multi-factor authentication	Still core, but fatigue makes it less dominant
4	Dark web monitoring	Behavioral biometrics	High concern about credential theft and resale
5	Geolocation & IP analysis	Dark web monitoring / Automated doc verification / Adaptive policies	Value in scalable, machine-driven checks

Today, the most used tools are multi-factor authentication (MFA), behavioral biometrics, and basic biometrics. These were easy to deploy, but they're not keeping pace with deepfakes and synthetic IDs.

The "perfect" IDV stack looks different. And there is a trick.

1. The Universal Anchor: Biometrics

Biometrics are the only tool that grows when firms design their "ideal" defenses, and the only one organizations stick with once adopted. They show the lowest drop-off rate and the highest pick-up rate of any technology, with 21% of non-users planning to add them. Aviation leads the charge, with 29% aiming to further expand biometrics, and Healthcare follows close behind at 26%. Even in Banking and Fintech, biometrics are being layered in as visible, trusted signals. The takeaway is clear: when companies prioritize simplicity, scalability, and user trust, biometrics win as the backbone of the future IDV stack.

2. MFA and Behavioral Biometrics: The Supporting Framework

MFA remains entrenched, especially in Banking, Crypto, and Healthcare. It's not disappearing but being re-framed: no longer the end goal, but a complementary layer. Although roughly a quarter of firms use behavioral biometrics (typing patterns, device interactions, mouse movement) today, adoption is shrinking in the ideal setup across nearly all sectors, from ~20–25% today to 10–20% ideally. Aviation in particular pushes the numbers down to near 11%, reflecting a preference for more proven or compliant tools. The conclusion is clear: MFA is steadily scaffolding, while behavioral biometrics are sliding into niche support.

3. Human Insight: A Local Spike

Human review rose sharply in the global averages, but this is not a universal comeback of manual checks. The spike is driven disproportionately by two markets—Germany and Singapore—where regulation, compliance culture, and risk sensitivity keep manual verification in play.

In compliance-sensitive scenarios, regulators require that a human decision-maker remains ultimately accountable for some high-stakes outcomes such as rejecting an onboarding application, freezing an account, or filing a suspicious activity report. This legal safeguard ensures that responsibility cannot be delegated entirely to an algorithm. At the same time, many jurisdictions mandate that consumers must have the right to appeal or contest an automated decision. Keeping humans in the loop provides that escalation path: if a customer challenges an outcome, there is a qualified person who can reassess the case, weigh context that the system may have missed, and issue a legally defensible final decision.

Outside of these markets, adoption is more modest, and the long-term trajectory points firmly toward automation and biometrics.

Table 3. Top 3 Tools by Sector: Current vs. Ideal

Sector	Current Top 3	Ideal Top 3
Aviation	Behavioral biometrics, Human review, Automated doc verification / Orchestration	Biometric verification, Geolocation and IP analysis, Adaptive policies
Banking	MFA, Biometric verification, Liveness detection / Human review	Biometric verification, Human review, MFA
Crypto	MFA, Geolocation and IP analysis, Behavioral biometrics / Automated doc verification	Biometric verification, Human review, Dark web monitoring / Checks against databases and watch lists / Orchestration
Fintech	Automated doc verification / Checks against databases and watch lists / Liveness detection, Orchestration/ MFA	MFA, Biometric verification, Adaptive policies / Automated doc verification
Healthcare	MFA, Behavioral biometrics, Automated doc verification	Biometric verification, MFA, Human review
Telecoms	Biometric verification, Fraud analytics, Behavioral biometrics	Checks against databases and watch lists/ Adaptive policies, MFA, Dark web monitoring

Industries highlight the split, building their own “sweet spot”:

→ Biometrics are the consistent winner: either current or aspirational #1 in almost every sector.

→ Human review is rising more strongly in Banking and Crypto, and in markets like Germany and Singapore, where compliance pressures are strongest. But outside of these, it’s not a universal top 3.

→ MFA remains strong everywhere, especially in Fintech and Healthcare, but is increasingly paired with biometrics rather than being standalone.

→ Behavioral biometrics & adaptive fraud alerts are rising in sectors chasing scale and customer experience (Aviation, Fintech, Telecoms).

→ Future setups are showing a pivot to biometric-first systems, backed by MFA and automation, with human-in-the-loop feedback selectively retained in compliance-heavy industries.

Also, the bigger the losses, the faster the pivot. High-fraud exposure firms are racing toward biometric-first setups, layering in behavioral checks. Exposure drives appetite: the more they lose, the stronger the push for proactive defenses.

The most widely deployed tools—MFA, behavioral biometrics, and basic biometrics—still play an important role, catching much of the low- and mid-level fraud. But against AI-driven attacks like deepfakes, synthetic IDs, and bot-powered credential stuffing, they fail if used in isolation. To stay ahead, firms must reset how they evaluate effectiveness—shifting from ease-of-deployment to resilience and building toward the “ideal stack”—biometric-first, powered by adaptive automation.

3 Reactive Metrics, Blind Spots Ahead

Table 4. Current vs. Desired Fraud Measurement Metrics – Top 5

Category	Metric	Nature of Metric	What It Measures
Current KPIs	Chargeback rate	Reactive	Captures financial harm already incurred
	Customer impact	Reactive	Measures scope of fallout once fraud hits customers
	Cost of fraud	Reactive/Strategic	Broad loss measure used in budget arguments
	Employee training effectiveness	Diagnostic	Tests internal readiness, not fraud outcomes
	False negatives	Diagnostic	Highlights system blind spots, informs model tuning
Desired Metrics	Compliance with regulatory standards	Compliance-driven	Keeps firms aligned with tightening laws
	Collaboration with external intelligence	Proactive	Builds early warning via shared threat data
	Fraud prevention ROI	Strategic	Proves investment value, wins budgets
	Customer satisfaction	Strategic	Links fraud defense to trust and retention
	Response time & fraud trend detection speed	Proactive	Measures agility in catching new schemes

Fraud programs are still measured by lagging indicators: chargeback rate, cost of fraud, and customer impact. These show how much was lost, not how well fraud was prevented. In contrast, the most requested KPIs are the fraud prevention ROI, detection speed, compliance and customer satisfaction.

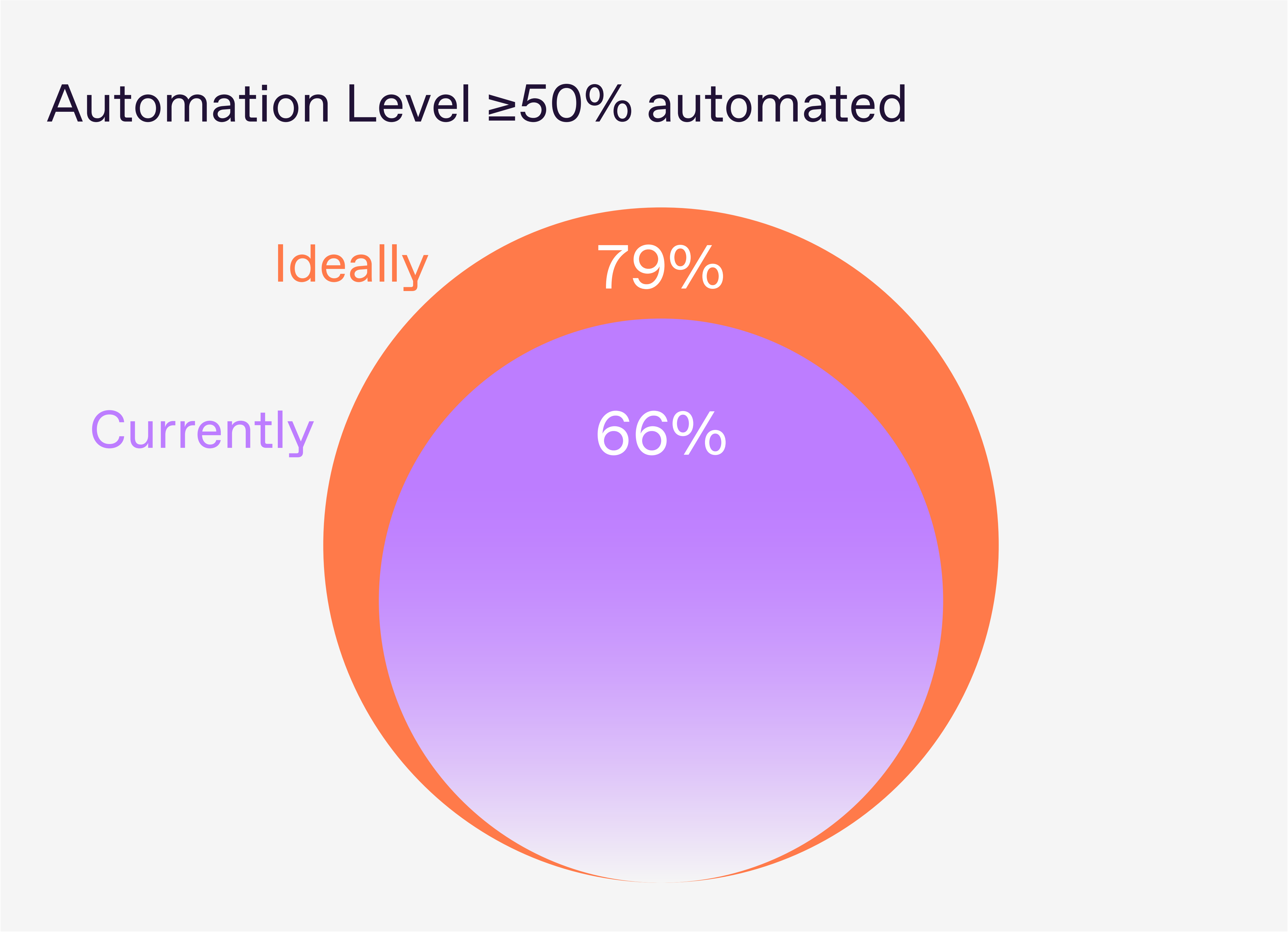
The shift depends on context. US firms emphasize ROI and customer trust (~18.5% each). Germany prioritizes satisfaction (20%) and intelligence sharing (18%). The UAE and Singapore stress compliance (~19%). Among very high-loss firms, response speed (25%) and trust (22%) are the top demands.

Firms might track outdated KPIs because regulators require them, finance teams default to familiar "loss" accounting, and prevention metrics like speed or false negatives are harder to standardize across departments. But as fraud moves higher on the board agenda, executives demand metrics that prove value creation, not just cost tracking. High-loss organizations (> $5M) are especially vocal: 25% name response speed as the most critical missing metric.

Fraud teams are being judged on yesterday's losses while boards want tomorrow's proof of resilience. Unless firms update KPIs to ROI, speed, and trust, they will struggle to not only justify budget growth or demonstrate strategic impact, but also to prevent fraud at scale.

4 The Automation Comfort Trap

Graph 3. Current vs. Ideal Levels of IDV Automation (Global)



Fraud is scaling faster than humans can handle. Companies openly admit that automated detection and response would be the most effective defense, yet many remain hesitant to push automation to its limits. Today, about two-thirds of organizations (66%) are already above the halfway mark on automation, but ideally nearly 4 in 5 (79%) want to be there. That's a 13-point gap pointing toward more machine-led defenses.

The "comfort zone" of 51–75% automation still dominates today, but its grip is weakening. More firms aspire to push into the 76–100% range, and even full automation is tripling in demand (from 3% today to 9% in the future). By clinging to mid-level automation, organizations give attackers an edge: fraudsters operate at machine speed, while businesses remain slowed by human bottlenecks. Encouragingly, the middle tiers are eroding as more companies reframe automation as not just efficiency, but survival.

Across industries, the ideal picture varies:

Healthcare is leaping ahead, with 53% of organizations now aiming for the 76–100% level of automation that only 17% have today.

Banking is polarized: nearly half are still sitting in their comfort zone (51–75%), but 11.9% are aiming for full automation, among the highest across sectors.

Aviation looks uneven, with 10% aiming for 0–25% automation while others push higher.

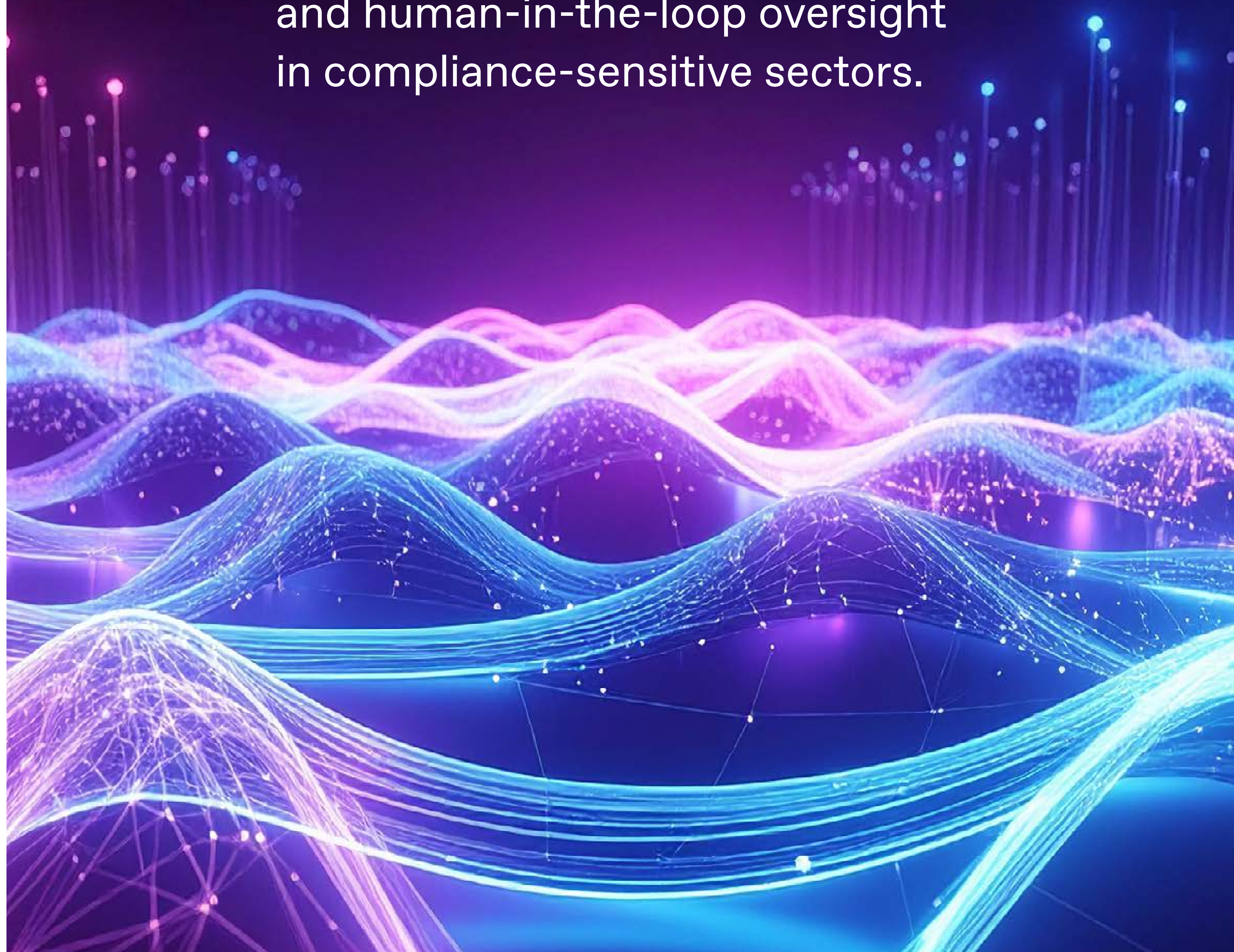
Fintech is the boldest, showing the highest appetite for full automation (12.5%) to support hyperscaling.

Crypto is already the furthest ahead in practice, with a quarter at 76–100% today, though adoption remains fragmented.

Telecoms show redistribution, shifting weight from the mid-zone into higher tiers: the share aiming for 76–100% automation rose from 23% to 31%, and full automation doubled from 2% to 6%.

Different industries push automation for different reasons: Healthcare needs compliance and data protection, Fintech needs efficiency and scale, Banking splits between cautious incumbents and bold challengers, Crypto reveals maturity gaps, Aviation is slowed by legacy systems, and Telecoms are accelerating to counter large-scale fraud.

The trajectory is unmistakably forward. While barriers like regulation and reputational risk still temper a full leap into automation, the data shows momentum is building. Organizations are steadily moving out of mid-range “comfort zones” and into higher tiers of automation, with full automation demand tripling. This reflects growing confidence that automation can be scaled safely when paired with orchestration platforms and human-in-the-loop oversight in compliance-sensitive sectors.



5 Training: Awareness Without Action

Table 5. Global Training Priorities: Current vs. Future

Rank	Currently in Place	Needed in Future
1	Basic awareness of AI-powered fraud techniques	Advanced ML & behavioral biometrics
2	Training on deepfake & synthetic identity fraud	Continuous learning on adversarial AI tactics
3	Red-teaming exercises against AI-generated fraud attempts	Regular simulations of AI-enabled social engineering

Our survey uncovers a critical imbalance in how organizations prepare their staff for AI-powered fraud. Today, training is still shallow and reactive. The majority of programs are focused on basic awareness (28%) and deepfake detection (26%)—important, but ultimately limited to recognition. Employees are being told what fraud looks like, yet they are rarely trained on how to respond when it strikes.

Only about a quarter of firms have progressed into deeper practices such as adversarial AI drills, ML-driven defenses, or red-teaming. These methods simulate the attacker's playbook and force teams to build the reflexes needed to contain damage. Even more concerning, nearly one in five organizations (18%) admit they have no structured training at all, leaving whole workforces unprepared in the face of fast-moving AI threats.

The future priorities named by respondents look radically different. Companies say their most urgent needs are advanced ML & behavioral biometrics (25%), continuous adversarial AI learning (25%), and social engineering simulations (25%). Unlike today's classroom awareness sessions, these approaches are hands-on and proactive. They shift the focus from recognizing fraud after the fact to anticipating and neutralizing it before damage occurs.

Training is evolving from a compliance-driven checkbox to a strategic defense capability. The next frontier is not about knowing the basics, but about engineering resilience—making sure employees can respond under pressure, adapt to new AI-driven attack vectors, and outpace adversaries who are constantly refining their tactics.

Opportunities: Where the Future Is Being Built

1 Biometrics Take the Front Seat

Biometric verification is moving to the center of fraud prevention. Today it ranks third in adoption, but in the ideal future stack it takes the top spot.

Three drivers may explain the rise:

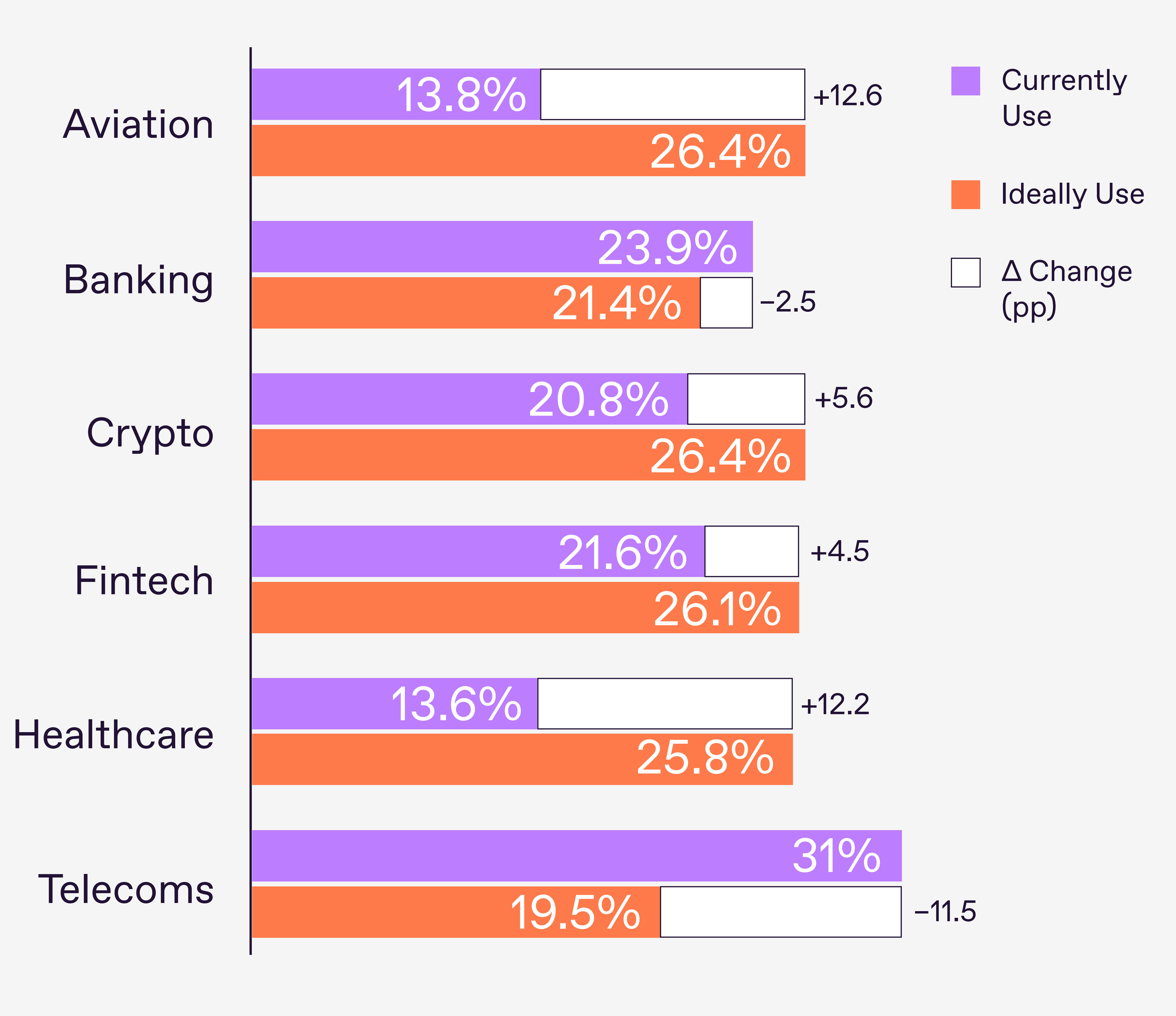
→ **User familiarity.** Face and fingerprint unlock are mainstream, reducing friction.

→ **AI defense.** Firms need liveness and PAD checks to counter deepfakes.

→ **Regulatory alignment.** Many sectors treat biometrics as regulator-approved "strong authentication."

The push is strongest in industries where identity fraud is tied directly to safety and compliance.

Graph 4. Biometrics Adoption Gap



Aviation and Healthcare show the strongest jumps, reflecting industries where trust and speed must coexist. Passengers already accept face scans at airports, and hospitals need quick but reliable staff/patient verification. Fintech and Crypto also move upward, betting on biometrics as part of a layered defense against synthetic IDs.

By contrast, Banking and Telecoms are actually dropping. Banking is shifting attention toward fraud analytics, dark web intelligence, and document and liveness checks. Banks may feel biometrics are already saturated or better handled with hybrid methods, while Telecoms—the current leader—may be reassessing reliance on face/fingerprint data, as they're wary of regulation and spoofing risks. Now, this sector is doubling down on compliance-driven and dynamic fraud prevention tools: watchlists, real-time alerts, and liveness.

Biometrics are climbing to the top of the wishlist, but not evenly. For some industries they're becoming the front door to trust, while for others they're just one piece in a layered defense.

2 Orchestration Platform: The Missing Link in Fragmented IDV

Table 6. What organizations need for effective management of multiple IDV tools and scenarios, top 5

Strategy	Biggest obstacles	Requirements	Alignment Insight
Integration	Integration issues across multiple vendors – 42.86%	Fully integrated ID verification solutions across vendors – 43.74%	Almost identical: fragmentation → demand for integration
Orchestration	Difficulty in automating and orchestrating – 43.21%	Automated orchestration of ID verification tools and workflows – 43.74%	Perfect mirror: orchestration gap → demand for automation
Cost Reduction	High costs from too many vendors/inefficiency – 38.10%	Reduced costs through vendor consolidation or tool integration – 43.39%	Direct alignment: cost obstacle → consolidation as solution
User Experience	Inconsistent UX across verification steps – 42.50%	Smooth, consistent user experience across verification steps – 40.92%	Both ~41%: friction → need for consistency
Speed	Verification delays/system slowness – 41.45%	Fast, real-time verification with no system delays – 38.80%	Perfect symmetry: delays → demand for real-time

For many companies, the top pain points are orchestration gaps and poor integration.

The picture shifts by region. US firms say fragmented journeys are the biggest issue (53%). Germany and Singapore point to integration failures (46%), while UAE companies struggle more with automation and orchestration (45%).

Sector patterns add more nuance. Fintech and Crypto firms suffer most from orchestration and UX gaps. Healthcare is an outlier, with 58% citing slow verification, held back by legacy systems. Banking emphasizes integration issues, while Telecoms complain most about poor user experience.

Table 7. Top 5 industry-level obstacles of effective IDV management, % of organizations

Obstacle	Aviation	Banking	Crypto	Fintech	Healthcare	Telecoms
Difficulty in automating/ orchestrating IDV	43.68	41.51	48.61	44.32	40.91	41.38
Lack of seamless integration	43.68	46.54	47.22	44.32	37.88	33.33
Fragmented user experience	44.83	37.74	45.83	50.00	34.85	45.98
Slow verification due to incompatibilities	39.08	44.03	38.89	32.95	57.58	37.93
High costs of managing vendors	34.48	41.51	36.11	32.95	34.85	41.38

This fragmentation is more than a nuisance—it is a systemic risk. Complexity slows verification more than fraudsters do. Every additional vendor, every manual workflow, every inconsistent customer journey adds delay and friction. Fraudsters thrive in these cracks: they exploit integration gaps, inconsistencies between tools, and the latency of manual review chains.

The market already recognizes the cure: orchestration platforms. A single layer that integrates tools, automates workflows, and standardizes customer experience is no longer a “nice-to-have”—it’s the missing link.

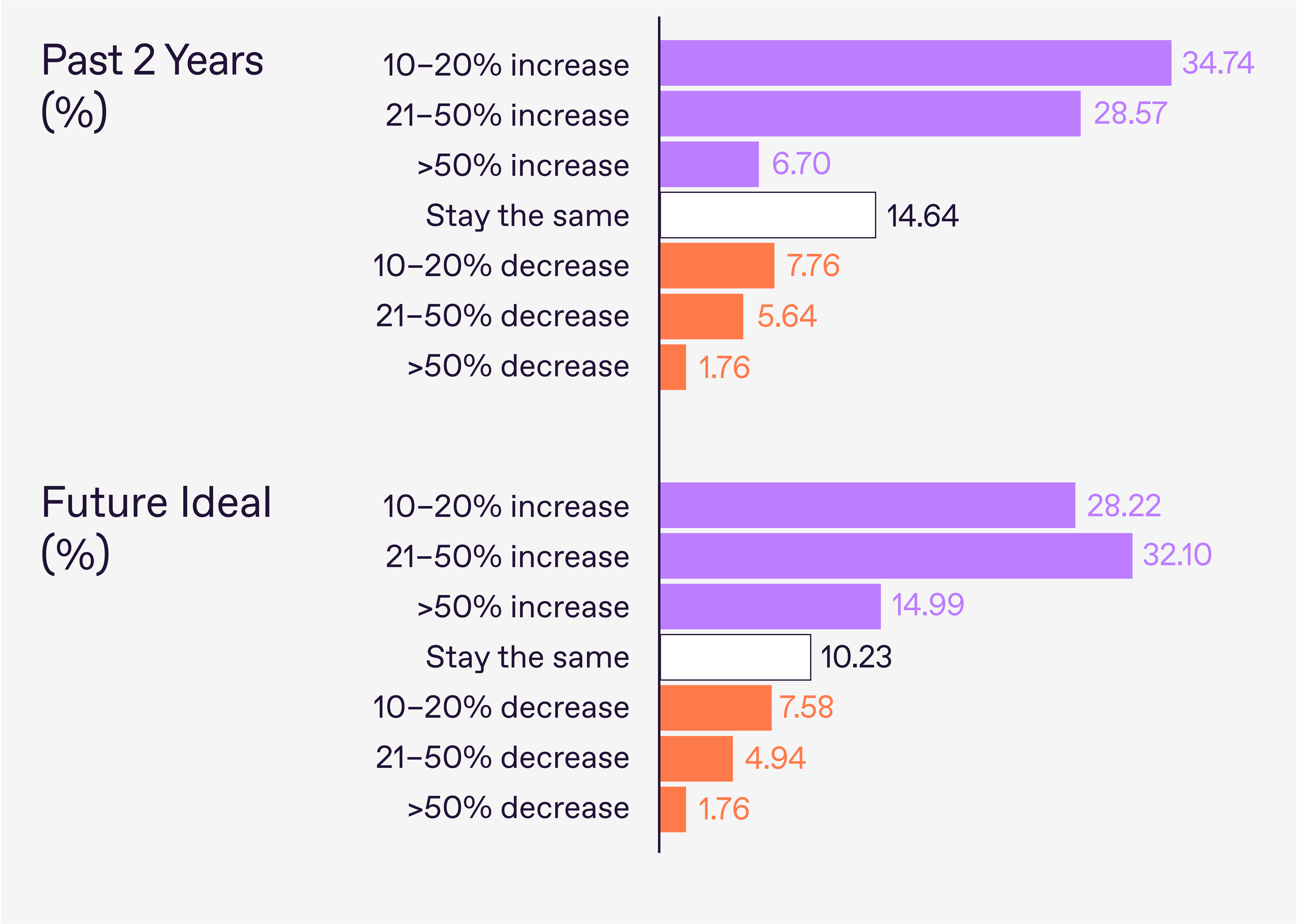
By consolidating IDV into a unified flow, firms can:

- → Cut costs through vendor reduction.
- → Improve user experience with smooth, consistent journeys.
- → Respond faster to fraud with real-time orchestration.
- → Reduce systemic risk by removing complexity itself.

ⓘ Fragmentation has become the new vulnerability. Organizations already know what they need—orchestration—but struggle to get there. The winners will be those who execute first, transforming IDV from a patchwork of tools into a coherent, resilient platform.

3 Budgets Are Shifting from Incremental to Exponential

Graph 5. Fraud Prevention Budgets: Past vs. Future (Global)



Budgets for identity verification and fraud prevention are exploding. In the past two years, almost two-thirds of firms grew spend, with 35% adding 10–20% and 29% adding 21–50%. Cuts were much more rare — only about 15% of organizations decreased their budgets.

The future looks even bolder. Almost one in three companies now want a 21-50% jump, and 15% are calling for more than 50%—triple the share that achieved such growth recently. Fraud prevention is no longer treated as an overhead—it's a frontline investment.

The drivers vary by who you ask:

→ **By geography:** The UAE, Singapore, and Germany are leaning toward mid-range growth, with about one-third of firms targeting 21–50% increases. The US shows a similar mid-range core but also stands out for its aggressiveness, with 22% of firms pushing for a 50%+ rise—the highest share globally.

→ **By sector:** Banking is stepping up—only about 4% of banks saw budgets more than double in the past, but now more than 15% say they want that level of increase going forward. Aviation shows a similar pattern: around 7% had huge jumps before, but 17% are now calling for them. Crypto, already a heavy spender, is also raising the bar—the share of firms planning to more than double their budgets has climbed from about 10% to 17%.

→ **By job role:** Leadership is driving the push for bigger budgets. Among Directors, the share calling for budgets to more than double has nearly tripled, from 7% to 18%, while 21–50% growth climbed from 31% to 34%. C-level executives are going even further: nearly one in five (19%) now want budgets to more than double, up from 7% in the past, and over a third (35%) are pushing for 21–50% increases. Together, these tiers reveal a leadership class intent on transformational spending.

ⓘ Across countries, industries, fraud loss levels, and job roles, the strongest gap is the appetite for a "more than 50% increase". The era of incremental growth is over. Budgets are shifting from "nice-to-have" increases to aggressive expansion, with executives treating identity verification as mission-critical infrastructure. The tension area now is whether fraud teams on the ground can keep pace with the scale of ambition being set from the top.

4 Redefining Responsibilities in Fraud Prevention

Table 8. What Teams Do vs. What They Should Do

Rank	Today's Top Responsibilities	Rank	Tomorrow's Top Priorities
1	Transaction monitoring & reviews	1	Employee training & awareness
2	Vendor due diligence	2	Adaptive prevention fraud policies
3	Legal/compliance work	3	Payment processing and transaction reviews
4	Employee training	4	Training ML models
5	Manual data entry and administrative tasks/ Payment processing and transaction reviews/ Ensuring compliance with KYC, AML, GDPR, etc	5	Investigating with forensics & analytics

Most fraud teams are stuck doing grunt work: watching transactions, chasing down disputes, filling out compliance forms. Necessary? Sure. But it's a defensive grind, and by the time you catch something, the damage is already done.

Ask practitioners where they want to spend their time, and the story changes. They point to building adaptive policies, training machine learning models, and running forensic investigations. That's not busywork, that's future-proofing. The shift is clear: fraud prevention has to move from manpower to brainpower, from reacting late to predicting early.

Sector Reflexes

Sector-level analysis reveals their fingerprints in how they fight fraud.

→ Aviation: Under-invests in forensic analytics (+14.9% gap compared to ideal state), while putting too much weight on customer disputes (–4.6%).

→ Banking: Shifting toward adaptive fraud policies (+6.3% gap) and business intelligence (+5.0%), as they see their over-investment in payment processing and review (–8.2%).

→ Crypto: Cutting back on employee training (–13.9%), while lacking data analytics and forensic techniques for investigation (+9.7% gap).

→ Fintech: Under-prioritizes legal collaboration (+5.7% gap) while over-investing in manual document verification (–9.1%) and customer dispute resolution (–8.0%).

→ Healthcare: Under-invests in legal investigations (+4.5% gap) and manual verification (+10.6%), while over-focusing on vendor due diligence (–9.1%) and forensic analytics (–7.6%).

→ Telecoms: Dramatically over-invests in transaction monitoring (–13.8% excess) and legal team collaboration (–8.4%), while under-developing employee training programs (+10.3% gap).

The bigger story is simple: everybody knows they need to get out of the weeds. Monitoring, compliance, paperwork—these are necessary, but they won't bend the fraud curve. The real opportunity is to free up resources, automate the grunt work, and shift human talent toward intelligence-driven defense. Fraud maturity isn't just about buying shinier tools, it's also about changing what people spend their time on—moving from "fraud janitors" cleaning up messes after they happen to "anti-fraud architects" building systems that prevent problems in the first place.

5 Identity Verification: From Tactical Checks to Trust Infrastructure

Table 9. Top 5 IDV Roles: Current vs. Future

Rank	Current Role of IDV	Percentage
1	**ML-powered systems** with biometrics, liveness detection, and risk-based verification	25.93%
2	Proactive with continuous **monitoring and AI-driven threat detection**	23.10%
3	Expected to be a **strategic enabler for trust and security** in business	22.40%
4	**Slow and costly** processes	21.69%
5	**Reactive to fraud and compliance** needs	21.52%

Table 9. Top 5 IDV Roles: Current vs. Future

Rank	Future Role of IDV	Percentage
1	**Fully integrated across all business functions** (marketing, customer service, personalized experiences)	26.81%
2	**Fully automated real-time verification with seamless, adaptive ML systems**	25.93%
3	**Global, near-instant verification with multi-platform support and effortless scalability**	25.04%
4	**Predictive security, adaptive to evolving threats and privacy laws**	24.69%
5	**Becoming the backbone of trust management in all digital and physical interactions**	24.16%

Identity verification is transforming from a necessary operational function into a strategic business enabler. This evolution reflects changing customer expectations and broader digital transformation trends, with organizations shifting focus from solving technical challenges to creating business value.

Today's identity verification priorities center on advanced technology implementation and operational problem-solving. Organizations are primarily focused on two areas—ML-powered biometrics and fully automated real-time verification—which together represent almost half of today's top priorities. Many companies are still working to establish proper governance structures across departments while dealing with fundamental efficiency problems like slow and costly processes.

The anticipated future reveals a very different approach. Organizations expect identity verification to become fully integrated across all business functions, serving as the backbone of customer experience rather than a standalone security tool. The emphasis is shifting toward global, near-instant verification capabilities that support international expansion and omnichannel customer experiences.

Future priorities also emphasize predictive security that adapts to evolving threats, moving from reactive fraud detection to proactive risk management. Organizations increasingly view identity verification as the foundation of trust management across all digital and physical interactions.

The significant change is the complete disappearance of operational challenges like "slow and costly processes" from future priorities, indicating organizations expect to resolve current inefficiencies and focus entirely on value creation. Cross-functional coordination, while important today, is giving way to seamless business integration as identity verification becomes embedded throughout organizations.

The shift toward predictive capabilities represents a move from fraud detection to fraud prevention, while the emphasis on global infrastructure shows companies planning for significant business expansion enabled by sophisticated verification systems.

Strategic Implications

Organizations today emphasize ML-powered biometrics and liveness detection (a top current practice). Looking ahead, this priority is evolving into a demand for fully automated, real-time verification with adaptive ML, which is projected to remain among the highest-ranked capabilities in the next 3–5 years.

The rise of full business integration as the top future priority signals that IDV strategies must align closely with overall business strategies. Organizations should begin planning how verification capabilities can enhance customer experience, enable new business models, and create competitive advantages.

The evolution toward predictive security suggests that risk management functions need to develop more sophisticated analytical capabilities and move beyond compliance-driven verification to business-enabling verification.

Conclusion

The data shows identity verification is undergoing a structural shift. Three dynamics stand out:

1

Automation Momentum

The majority of firms are already past the halfway mark on automation, and demand is building to push further. The “comfort zone” of mid-level automation is eroding as companies move decisively into higher tiers. This reflects not hesitation but growing confidence that automation can be scaled safely, provided it is combined with orchestration and regulatory safeguards.

2

Local vs. Global Patterns

Some global averages are distorted by local effects. The rise in human review, for example, is a regional anomaly driven by Germany and Singapore, where compliance frameworks require human accountability. Outside these markets, adoption is modest and the trendline points firmly toward automation and biometrics. This underlines that global narratives must be read through a regional lens, with regulation acting as a key variable.

3

From Tools to Systems

The fragmentation of IDV stacks—multiple systems, inconsistent UX, and manual workflows—has become as dangerous as fraud itself. The clearest through line across industries is that point solutions no longer suffice. Organizations know the answer: they need orchestration platforms that unify tools, remove inefficiencies, and enable end-to-end automation.

Taken together, all these findings suggest that the future of IDV is orchestrated automation, not incremental layering. Manual oversight will not disappear, but it is being reframed as a narrow compliance function rather than the operating model.

For organizations, the strategic challenge is no longer whether to automate, but how quickly they can consolidate fragmented systems into a single orchestrated backbone of trust.

About Regula

Regula is a global leader in identity verification, with forensic science at our core. For more than 30 years, we've been building solutions that validate identities for banks, businesses, and border agencies worldwide. Long before identity fraud became today's massive threat, we were setting the standards for how to detect and stop document fraud—and today, we provide the backbone of digital trust.

What Makes Us Different

- Forensic DNA: Three decades of forensic expertise built into software—detecting manipulations and tricks other systems miss.
- Proprietary solution: Hardware and software solutions for identity document verification, biometrics, identity lifecycle management, and orchestration—all built in-house. Faster, integrated, secure.
- The largest and most comprehensive document database: 15,500+ templates from 254 countries and territories, covering every detail of a document—numbers, fields, fonts, dynamic security features (holograms, OVD/OVI, MLI, etc.), MRZ/barcodes, chip data, and other.
- One-stop shop: End-to-end identity verification without stitching together multiple vendors.
- Data Control: Flexible deployment (on-prem, cloud, hybrid) for compliance and security.

Contact Information pr@regulaforensics.com
regulaforensics.com