OCTOBER 2024

IDverse™

IDV GUIDE FOR FINANCIAL SERVICES

UNMASK DEEPFAKES

Table of Contents

Introduction

This ebook is tailored for financial services professionals, aiming to provide a comprehensive understanding of virtual identity verification (IDV). It explores key concepts, technologies, and best practices to equip readers with actionable insights for implementing secure and user-friendly IDV solutions.

Identity verification trends within the financial sector include the adoption of reauthorization and advancements in liveness detection using artificial intelligence (AI). Additionally, AI-driven fraud detection methodologies are being leveraged to combat sophisticated threats like deepfakes and synthetic identities while verifying the authenticity of government-issued documents during onboarding.

To cater to the growing demand for mobile banking as well as for secure account access recovery, companies are developing and optimizing mobile-first biometric solutions, and regulatory compliance is a key focus to ensure alignment with evolving requirements such as GDPR, CCPA, and PSD2, among others.

This guide explores the significance of trusted identity solutions and the increasing need for collaboration between AI-powered IDV companies and the financial sector in the following chapters:

1. Why Virtual IDV is Crucial for Financial Services

In the contemporary digital economy, virtual identity verification has become a necessary component for financial services providers. Indeed, with more consumers than ever embracing online and mobile banking, investment platforms, and digital payment solutions, the need for secure, reliable, and user-friendly IDV methods has never been more important.

The landscape is fraught with risk; financial institutions must navigate a complex web of regulatory requirements, fraud prevention measures, and customer expectations while ensuring a seamless user experience.

The significance of IDV for financial services

Below are some of the key reasons why offsite identity validation has become an indispensable component of financial services:

- **Regulatory compliance**: The financial services sector is subject to stringent regulations designed to prevent money laundering, terrorist financing, and other illicit activities. Virtual IDV plays a vital role in helping financial institutions comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Robust IDV solutions allow financial services providers to verify the identity of their customers, assess risk levels, and fulfill their regulatory obligations.
- **Fraud prevention**: With trillions of dollars' worth of assets under management, financial services providers are prime targets for fraudsters seeking to exploit vulnerabilities in digital systems. Virtual IDV acts as a powerful deterrent against fraud by ensuring that only legitimate customers can access financial accounts and services. Through the use of advanced technologies such as biometrics, machine learning (ML), and artificial intelligence, financial

institutions can detect and prevent fraudulent activities, protecting both their customers and their own reputations.

- **Customer experience**: In the highly competitive financial services industry, customer experience can be a key differentiator. Online IDV enables financial institutions to onboard new customers quickly and efficiently, without the need for in-person visits or extensive paperwork. Providing a streamlined, user-friendly IDV process permits financial services providers to enhance customer satisfaction, build trust, and develop long-term relationships with their clients.
- **Operational efficiency**: Implementing virtual IDV solutions can significantly improve operational efficiency for financial services providers. By automating the identity verification process, financial institutions can reduce manual workload, minimize errors, and accelerate onboarding times. This not only saves time and resources but also allows financial services providers to scale their operations more effectively, accommodating growing customer demand without compromising on security or compliance.

It's plain to see that strong online IDV solutions, if properly implemented, have the ability to ensure that financial organizations can accurately verify customer identities, assess risk levels, and fulfill their regulatory obligations.

Challenges for IDV within the financial services sector

Implementing effective virtual identity solutions in the financial services sector is not, however, without its challenges. Financial businesses must navigate complex regulatory terrain, evolving security threats, customer expectations, and data privacy concerns to ensure the success of their initiatives.

Some of the challenges include the following:

- **Balancing security and user experience**: One of the primary challenges facing financial services providers is striking the right balance between security and user experience. While robust IDV measures are essential for preventing fraud and ensuring compliance, overly complex or time-consuming processes can frustrate customers and lead to abandonment. Financial institutions must carefully design their IDV workflows to minimize friction while maintaining the highest levels of security.
- **Keeping pace with evolving threats**: Fraudsters are continually developing newer and more sophisticated methods to circumvent IDV controls. Financial services providers must stay ahead of these threats by investing in advanced technologies and collaborating with industry partners to share intelligence and best practices. Success in this realm requires a proactive, agile approach to IDV that can adapt to changing risk landscapes and emerging attack vectors.

> 25% of all fraudulent documents we're stopping now is synthetic media, that is, created by generative AI.
>
> PAUL WARREN-TAPE, IDVERSE

- **Ensuring inclusivity and accessibility**: Financial inclusion is a critical goal for the sector, and virtual IDV solutions must be specifically designed with inclusivity and accessibility in mind. This means accommodating a diverse range of

customers, not just with respect to age, gender, and ethnicity, but also including those with disabilities, limited access to technology, or non-traditional identification documents. Financial institutions must engage with IDV solutions that are intuitive, user-friendly, and accessible to all, ensuring that no customer is excluded from accessing essential financial services.

- **Navigating data privacy concerns**: As financial services providers collect and process sensitive personal information for IDV purposes, they must encounter a challenging landscape of data privacy regulations and consumer concerns. Compliance with laws such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) requires financial institutions to be transparent about their data practices, obtain customer consent, and implement strong data protection measures. Building and maintaining customer trust in the IDV process is essential for the success of online IDV in the financial services sector.

Virtual IDV is a critical enabler for the financial services sector, helping institutions comply with regulations, prevent fraud, enhance customer experience, and improve operational efficiency.

It's important to remember, however, that implementing effective IDV solutions requires careful consideration of the challenges involved, including balancing security and user experience, keeping pace with evolving threats, ensuring inclusivity and accessibility, and navigating data privacy concerns.

Challenges & Mitigation for IDV in the Financial Sector

Challenge	Description	Mitigation Strategies
Fraudulent Activities	Increase in sophisticated fraud attempts such as identity theft, synthetic identities, and account takeovers	• Implement multi-factor authentication (MFA) and biometric verification. • Use advanced fraud detection systems powered by machine learning and AI.
Data Privacy & Security	Ensuring sensitive customer data is protected against breaches and misuse	• Employ end-to-end encryption and secure data storage • Adhere to regulatory frameworks like GDPR, CCPA, and other data protection laws
Regulatory Compliance	Staying compliant with evolving regulations like AML, KYC, and CDD	• Regularly update compliance programs and ensure staff training on regulatory changes. • Use automated compliance solutions that integrate with identity verification processes.
User Experience & Accessibility	Balancing robust security measures with seamless and user-friendly processes	• Design intuitive and simple verification processes • Provide multiple verification options (e.g., mobile, online, in-person) to cater to different user preferences
Cost of Implementation	High costs associated with deploying advanced identity verification systems	• Opt for scalable and modular verification solutions that can grow with the business • Leverage cloud-based services to reduce infrastructure costs
Integration with Existing Systems	Ensuring new identity verification solutions integrate seamlessly with existing financial systems	• Conduct thorough planning and testing before implementation • Choose solutions with flexible APIs and strong support for integration
False Positives & Negatives	High rates of false positives or negatives in identity verification can lead to customer frustration	• Continuously improve algorithms and data quality to enhance accuracy • Implement manual review processes for suspicious cases
Global Reach & Scalability	Verifying identities across different countries with varying documentation and verification standards	• Use global verification solutions that support a wide range of documents and languages • Partner with local verification service providers in regions with specific requirements

Technological Advancements & Adaptation	Keeping up with rapidly changing technology and potential obsolescence	• Invest in adaptive and upgradable technology platforms • Stay informed about the latest trends and innovations in identity verification technologies
Social Engineering & Phishing Attacks	Exploitation of human behavior to bypass verification processes	• Educate customers and employees on recognizing and avoiding phishing and social engineering attacks • Implement email and SMS filtering solutions to detect and block phishing attempts
Digital Identity Gaps	Discrepancies or lack of digital identity information for certain segments of the population	• Develop alternative verification methods that do not solely rely on traditional digital footprints • Collaborate with governmental and non-governmental organizations to enhance digital identity coverage
Third-Party Dependency	Reliance on third-party providers for identity verification services	• Conduct due diligence and regular audits of third-party providers to ensure compliance and reliability • Maintain backup verification processes to mitigate risks associated with third-party service interruptions

IDV in the financial services sector faces a multitude of challenges, ranging from sophisticated fraud attempts and data privacy concerns to regulatory compliance and technological advancements. Mitigation requires a multifaceted approach that incorporates advanced technologies like AI and machine learning, robust security measures such as multi-factor authentication and encryption, and seamless integration with existing systems.

Additionally, maintaining a balance between stringent security protocols and user-friendly processes is crucial for enhancing customer experience. Staying adaptable to technological changes, investing in scalable solutions, and fostering collaboration with regulatory bodies and local verification providers are practices that permit financial institutions to effectively address these challenges, ensuring secure and efficient identity verification processes.

2. An Overview of Identity Verification

It is difficult to overstate the importance of implementing trusted identity solutions in contemporary society. With some of the most onerous compliance requirements of any industry and trillions of dollars to manage, the financial sector in particular has a heightened responsibility with identity.

To tackle the complex challenges posed by identity fraud and unauthorized access to sensitive information, a collaborative effort between AI-powered IDV software companies and financial services companies has become imperative.

Fundamentals of identity verification

Most businesses rely heavily on documents produced by a range of government agencies to help identify their customers. Ultimately, there are two key questions that individuals must confidently answer to prove their identity:

1. **Are you a real person?**
2. **Are you the right person?**

Traditionally, organizations seeking to verify identities relied heavily on manual processes and physical documents. People seeking verification would present paper-based credentials such as IDs, passports, or driver's licenses. Verification agents then manually compared the presented documents with their physical appearance and information stored in databases. This process, while widely used, was prone to various risks and vulnerabilities.

Forgery was a significant concern, as skilled counterfeiters could produce convincing fake documents. Of course, under these circumstances, identity theft was rampant. Stolen or lost documents could be used by criminals to impersonate others, leading to the defrauding of businesses and other serious violations.

Unsurprisingly, human error was also prevalent. Mistakes in document examination or database entries were common, frequently resulting in instances of wrongful verification or denial. The reliance on paper documents made the system susceptible to loss or damage, further compromising its reliability. Additionally, the manual nature of traditional identity verification often led to delays and inefficiencies, particularly in high-traffic environments like bank branches. Long queues and slow processing times were far from unusual.

As the digital landscape expanded, the need for advanced, secure, and reliable identity verification solutions became paramount to maintain the integrity of online interactions.

The era of generative AI begins

Today, AI-powered identity verification systems are rapidly replacing conventional methods. Unlike paper documents, IDV solutions backed by AI verify identities through methods such as facial recognition, fingerprint scans, and voice analysis. Machine learning algorithms detect anomalies within ID documents, while automation accelerates the process from start to finish. This shift signifies a transformative advancement in identity verification, enhancing trust and safeguarding against modern threats.

The highest-quality modern identity verification systems work using facial biometrics and perform the following key identity proofing steps in an automated manner using AI:

1. **Optical character recognition (OCR)**: The software uses adaptive text recognition and extraction for ID document data validation as well as easy form autofill for the end user.
2. **Document fraud analysis (DFA)**: Dozens of data checkpoints are used to perform an analysis and verify that the ID document is in fact authentic and present at time of verification.

3. **Anti-spoofing**: An automated facial biometrics match is performed on the selfie captured in the liveness video against the face image on the identity document.
4. **Liveness detection**: Advanced, automated checks are made on the face capture mini-video which can detect print attacks, masks, screens, and deepfakes—including both presentation and injection attacks—and which includes depth perception, miniscule movements from heartbeat, and light refraction.

> A human manual reviewer may have a bad morning before work — an argument with their spouse, cut off in traffic whilst commuting — and these factors have an effect on their decision making which a neural network does not.
>
> MATT INGMAN, IDVERSE

These four key checks make AI-backed IDV solutions indispensable for financial services businesses seeking to reliably authenticate the individuals with whom they are interacting—but as we'll see in the next chapter, not all machine learning algorithms are created equally.

3. The Evolution of IDV Systems

In an era where digital interactions predominate, verifying identities in real time is critical for ensuring security and building trust. Whether opening an online account, obtaining a loan, or securing bank employees' access, confirming an individual's identity is essential.

This chapter explores the progression of identity verification solutions, from rudimentary passwords to cutting-edge, automated systems enabling instantaneous identity confirmation.

Passwords' long reign

Passwords were introduced in the 1960s as a means of securing early computer systems, with origins at the Massachusetts Institute of Technology (MIT). Computer scientist Fernando Corbató is credited with first using them to protect file access on the large computer systems he was working on at the time.

For decades, passwords remained the primary method for knowledge-based identity verification and access control. Their low implementation cost kept passwords dominant despite security weaknesses like guessability, replay attacks, and phishing. Passwords persist today, but—as Corbató himself acknowledged later in his career—this elementary security measure is no longer adequate on its own. Improved technology now augments their security limitations.

In the US, the Social Security number (SSN) was also introduced as a knowledge-based solution, used in tandem with passwords. However, the proliferation of SNNs' use as a personal identifier, coupled with security breaches that have exposed most of the confidentiality associated with the numbers, have substantially diminished their reliability.

ID verification emerges

At its core, knowledge-based password authentication represents primitive identity verification—an individual wants to access information, so they must know the right combination of letters, numbers, and symbols that prove they are someone authorized to have that access.

Early identity verification relied extensively on manual processes like in-person verification, physical documents, and knowledge questions. While functional, these methods were inefficient, prone to human error, and provided poor user experiences. Technology innovations soon aimed to enhance identity proofing.

The rise of biometrics

The past thirty years have seen the emergence of attribute verification to enhance identity verification. A person's personal attributes, such as one's fingerprints or face, are generally regarded as the most secure verification method subject to maintaining strong presentation attack defenses in the technology to avoid hack attempts.

Fingerprint recognition gained prominence in the 1990s as one of the earliest biometric authentication methods. Face recognition followed in the 2000s, relying on facial structure analysis for identification. Mobile devices accelerated the adoption of attribute biometrics to manage control over personal data in the event of a lost or stolen device.

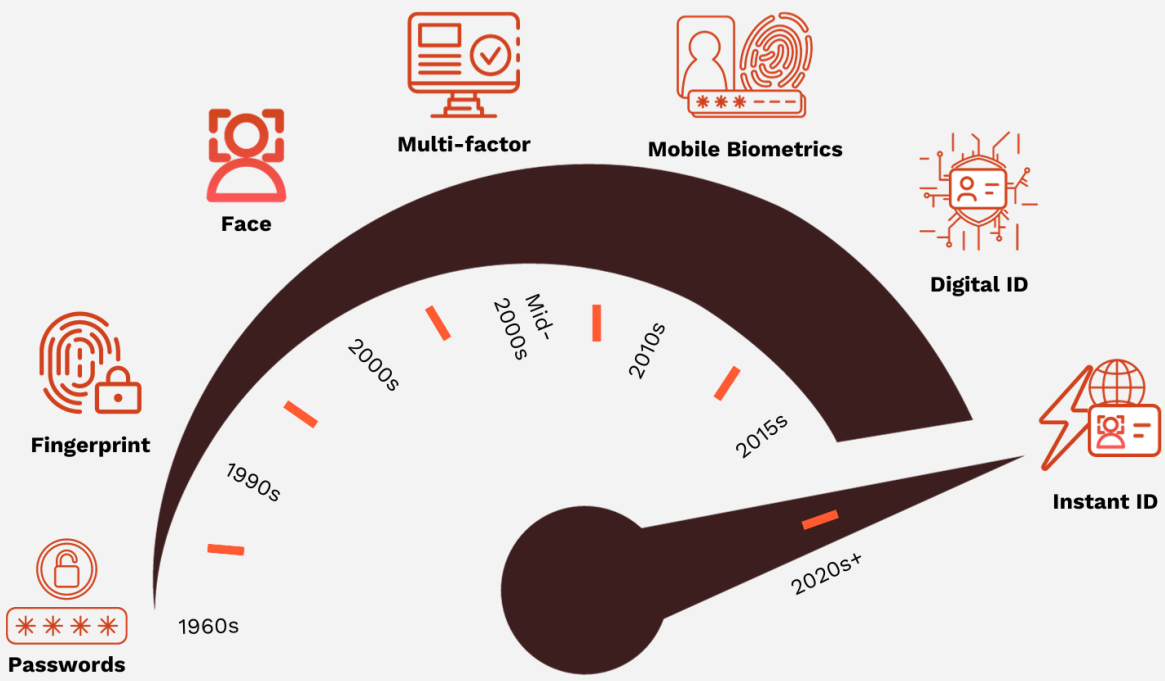
Today, the Australian government's cyber team advises all government websites to use biometrics rather than username and password for logging in. (See Principle 5 in this link.)

Multi-factor & decentralized identity

By the 2000s, multilayered security became best practice. Multi-factor authentication (MFA) combines different layers of

authentication, including knowledge, device, and attribute methods.

Biometrics are considered the strongest form of MFA, with additional factors like passwords and tokens for layered security. The 2010s saw major advancements in decentralized digital identity via blockchain and self-sovereign identity solutions to increase user control.



Instant identity starts now
The evolution of computer vision technology has changed the identity verification landscape and simplified user experience.

The future is Instant ID

More recently, the COVID-19 pandemic accelerated the use of virtual identity verification and digital IDs for access to services. The automated IDV solutions of the present day use

state-of-the-art tech like artificial intelligence (AI) and machine learning (ML) to verify identities in seconds.

Contemporary leading identity verification techniques converge passwords, biometrics, multi-factor authentication, and integration with authoritative identity data sources into instant, seamless verification that is both highly secure and universally interoperable.

Instant identity is the result of this convergence—made possible through advancements in the underlying technologies—and has not only simplified the user experience, but increased the overall security of identity verification. As the technology progresses, instant identity verification will likely become ubiquitous across digital interactions, powering frictionless, trusted authentication.

4. Eliminating Bias, Embracing Inclusion

The financial services sector has a key role to play in promoting inclusivity and eliminating bias within their organizations and the broader society they serve. In prioritizing these values, companies can ensure that all individuals, regardless of age, gender, or ethnicity, have equal access to financial opportunities and resources.

On the employment side, studies have demonstrated time and time again that diverse and inclusive workplace environments drive innovation, improve decision-making, and enhance overall business performance. When employees from various backgrounds and experiences collaborate, they bring unique perspectives and ideas to the table, leading to more creative solutions and better outcomes for the company and its clients.

Eliminating bias is therefore not only an ethical imperative but also a sound business strategy. Removing bias, in its myriad forms, from the IDV procedure should accordingly be a top concern for financial services businesses everywhere.

Bias here & there

Identity verification processes can be marred by various biases, undermining their fairness and accuracy. The four key sources of bias within verification systems are: system bias stemming from unequal access to technology; algorithmic bias; data bias, influenced by skewed datasets; manual screening bias, arising from human judgments; and language bias, driven by linguistic nuances.

Let’s examine each one in a bit more detail:

- **System bias**: If an identity verification solution only works on the latest smartphone model with a superior camera spec or with a high speed internet connection, then any users who do not meet these requirements will be forced to rely on manual methods of verification or be excluded from accessing a service altogether.
- **Algorithmic bias**: When improperly designed, the coded rules embedded within an algorithm itself can inherently favor or discriminate against certain groups. Mitigating this bias involves addressing programming decisions to prevent unjust outcomes independent of training data.
- **Data bias**: If biased data is used to train the algorithm, it is likely the system will exhibit those same biases when making decisions. This has become the AI industry's Achilles heel. Advancements in generative AI, also known as synthetic media, combined with ethically-sourced synthetic datasets for training shows that developers are using this tech to make their products better.
- **Manual screening bias**: Automated IDV systems that are available at all times, day or night, and require no manual human intervention are far more inclusive to a wider customer base. For example, offering account opening services during business operating hours, when human analysts are available, excludes low-income customers who can't afford to take time off of work.
- **Language bias**: The onboarding process often represents a major hurdle to users, who are prepared to drop off if this stage is too difficult or can't be completed. Removing the barriers that prevent users from comprehending the actions they need to successfully advance through each stage requires catering to a range of accessibility needs.

Countering bias

To face these challenges head on, IDVerse has introduced the Code Zero Bias Oath, inspired by the enduring principles of the Hippocratic Oath, but tailored to the unique challenges and

opportunities of the field of AI-powered biometric identity verification technology. This oath embodies a commitment to reducing algorithmic bias, promoting fairness, and upholding the highest ethical standards in AI software development:

Code Zero Bias Oath

I, as a creator of AI technology, solemnly swear to uphold the principles and practices outlined in this Code Zero Bias Oath. In my pursuit of designing, developing, and deploying software, I commit to the following:

***Do No Harm**: I shall prioritize the well-being of individuals and communities who may be affected by the software I create. I will strive to ensure that my work does not cause harm or perpetuate bias, discrimination, or inequality.*

***Equity and Fairness**: I will actively seek to identify and rectify biases in algorithms and data sets. I pledge to promote fairness and impartiality, striving to create software that treats all individuals equally regardless of their background, race, gender, or any other characteristic.*

***Transparency and Accountability**: I will be transparent about the decision-making processes and data sources used in my software. I accept responsibility for the consequences of my work and will be accountable for any biases or ethical lapses that may arise.*

***Inclusivity**: I will advocate for diverse and inclusive teams, recognizing that different perspectives lead to more robust and ethical solutions. I will actively work to create an environment where underrepresented voices are heard and valued.*

***Continuous Learning**: I understand that technology evolves rapidly, and I commit to staying informed about emerging best practices, guidelines, and regulations related to algorithmic bias and ethical software development.*

***User Privacy and Consent**: I will respect user privacy and seek informed consent for data collection and usage. I will implement strong data protection measures to safeguard user information.*

***Mitigation and Remediation**: If I discover bias or ethical concerns in software I have developed, I will take immediate steps to mitigate harm and rectify the issues. I will report such concerns to relevant stakeholders and take corrective action.*

***Community Engagement**: I will actively engage with the communities impacted by my software, seeking their feedback and addressing their concerns. I will be open to criticism and commit to improving my*

work based on community input.

***Regulatory Compliance**: I will adhere to all relevant laws, regulations, and industry standards related to algorithmic fairness and data ethics in software development.*

***Advocacy for Ethical Technology**: I will advocate for the responsible and ethical use of technology within my organization and the broader industry. I will use my influence to promote ethical practices and raise awareness about the importance of reducing algorithmic bias.*

I acknowledge that my work as an AI technology creator has a profound impact on society, and I accept this oath as a solemn commitment to ethical software development. I will strive to uphold these principles throughout my career, recognizing that my actions can shape the future of technology and its impact on humanity.

*By taking this **Code Zero Bias Oath**, software engineers demonstrate their dedication to ethical software development, with a focus on reducing algorithmic bias and promoting fairness, transparency, and accountability.*

By taking this Code Zero Bias Oath, makers of AI technology demonstrate their dedication to ethical software development, with a focus on reducing algorithmic bias and promoting fairness, transparency, and accountability.

Table of identity verification certifications

The table below covers key identity verification and security certifications from government entities, international standards bodies, and industry organizations. These trustmarks validate compliance with best practices for protecting sensitive personal data, managing risk, ensuring reliability of biometric systems, minimizing bias, and providing assurance through independent auditing.

Certifications for IDVerse

Certification body	Basic certifications	Advanced certifications
NIST	NIST SP 800-171	NIST SP 800-53 NIST SP 800-63 IAL 2
iBeta/BixeLab against ISO 30107-3	Liveness PAD Level 1	Liveness PAD Level 2 Liveness (bias testing)
Government entities	CPRA GDPR	TDIF L3 DIATF
ISO (International Organization for Standardization)	ISO 27001 ISO 9001 ISO 19795	ISO 22301 ISO 27017 ISO 27018 ISO 27701 ISO 29100 ISO 30107-3
AICPA System and Organization Controls (SOC)	SOC 1	SOC 2

5. Meet IDVerse

It's probably time that we tell you a bit more about ourselves. We're IDVerse, and we let businesses scale globally through our automated, AI-powered identity verification solution.

With our technology, private enterprises and governments alike can verify new users in seconds with just a face and a smartphone. Our technology is capable of recognizing over 16,000 identity documents from over 220 countries and territories in over 140 languages and typesets.

No other solution in the market has this level of global coverage.

We empower true identity for people around the world. Through our quest for Zero Bias AI™-tested technology, we pioneered the use of generative AI to train deep neural network systems to protect against discrimination based on race, age, and gender. Through our advancements in the field of natural vision processing (NVP), we're teaching machines to autonomously see and perceive like humans, and excel in ways that people cannot.

A brief history of our company

Our founders, Dan Aiello and Matt Adams, started out coding retail commerce apps. They wanted to develop a smooth, one-click experience for online account opening, purchasing, and checkout. Identity verification was crucial for this to happen, but none of the available technology worked well enough. It was also during this time that computer vision and machine learning were becoming viable technologies.

Dan and Matt thus focused their energy on tackling the problem of using modern machine vision to let people positively and easily prove their identity. Thus the idea of autonomous identity verification was born. IDVerse—then known as OCR Labs—opened its doors in Sydney, Australia in 2018.

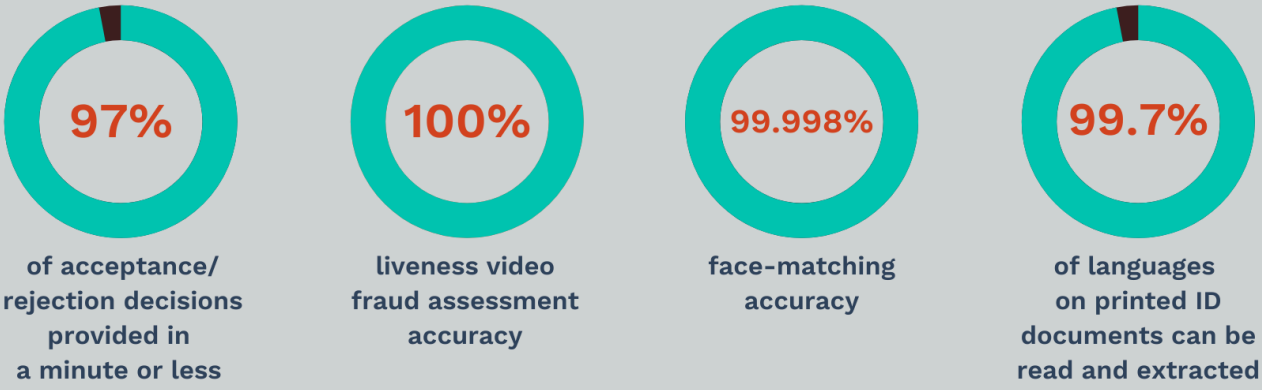
The solution

IDVerse provides the foundational technology and infrastructure to enable businesses of all sizes and sectors to conduct robust identity verification. Our flexible, modular approach allows companies to tailor their IDV solutions, whether they require individual components, custom configurations, or comprehensive end-to-end systems. We offer an API layer that allows you to consume data downstream, with the entire process being fully automated.

Our core capabilities include:

- **Document verification**: Customers can verify an ID document and onboard users safely from anywhere in the world. Our solution "sees" and interprets documents, rather than relying on templates.
- **Biometric verification**: Our tech allows our customers to know it's a live person presenting an ID document and that it's their face in the document image. Advanced image analysis and liveness checks spot real users making a genuine attempt to sign up.
- **Data verification**: OCR technology extracts information from an ID document and verifies it against local government and credit bureau databases—all in real time. This capability allows our customers to meet compliance obligations.
- **Face Access**: Step-up authentication keeps users' accounts secure and makes account recovery easy by matching their face to their original ID, which they provided during onboarding.
- **FraudHub/blocklist**: An extra layer of fraud detection helps identify recurring fraudsters or identity theft velocity attacks, ensuring they are flagged in future interactions.
- **Proof Of Address**: Scan any printed A4 document to extract the address, date, and other key details to match against either supplied data or an ID document.

Unrivaled accuracy & performance

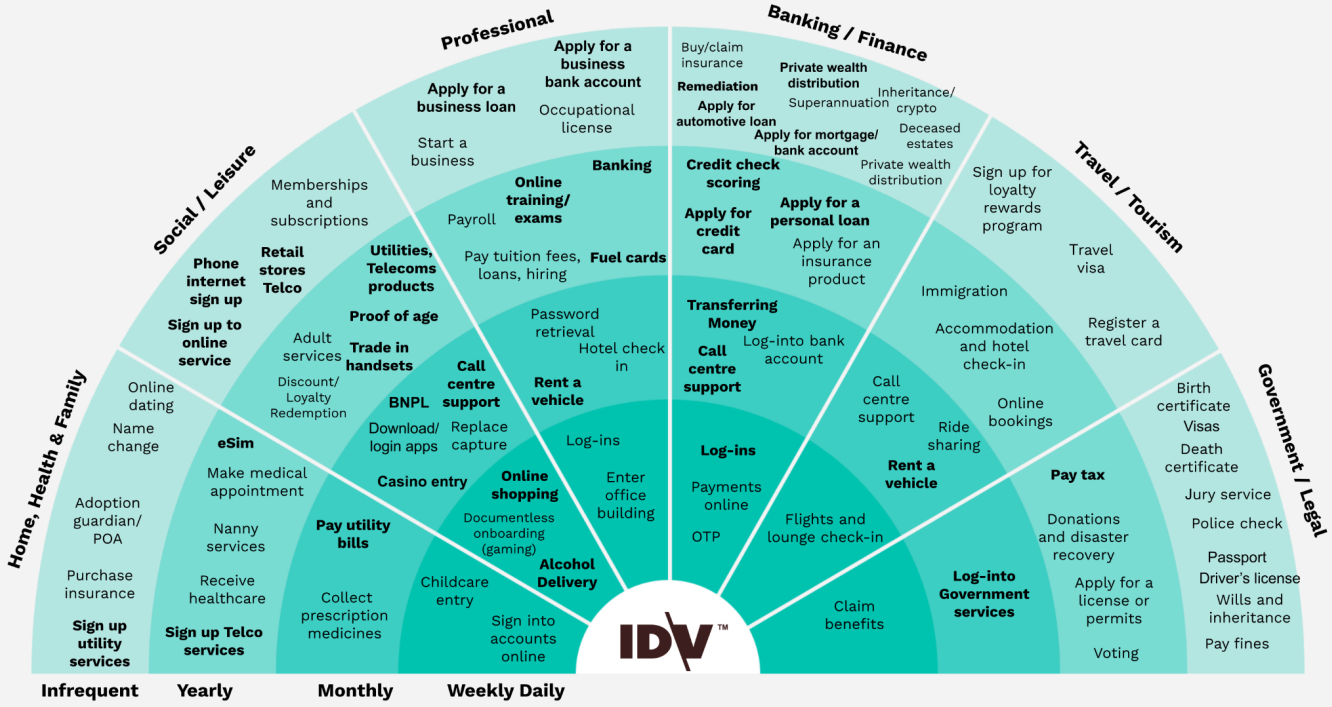


Any or all of these modules can be seamlessly integrated to power solutions across the cybersecurity, authentication, and compliance spectrum. Whether you're in financial services, gaming, healthcare, or any industry requiring secure identity verification, IDVerse provides the tools to build trust in your digital ecosystem.

From SMBs and startups to enterprise-level organizations, IDVerse enables businesses to achieve the following:

- **Enhance fraud prevention**
- **Streamline user onboarding**
- **Meet regulatory compliance**
- **Improve risk management**
- **Strengthen cybersecurity measures**

Our SDKs give you the flexibility to make our technology the cornerstone of your IDV strategy regardless of your specific needs or use case. The IDVerse solution is trusted by customers in a wide range of verticals including:



The IDVerse solution is trusted by customers in a wide range of verticals including:

6. IDV Use Cases in Financial Services

Identity verification technology, now backed by the power of Zero-Bias AI™, has solidified its place as a paradigm-shifting force within the financial services sector. Its applications extend far beyond mere identity confirmation, including account opening and access, customer support authentication, employee access control, and more.

Below, we take a deeper dive into how financial businesses are leveraging IDV software to create a more efficient, secure, and equitable future for all clients.

Financial Services Sector Use Cases

Use Case	Description
TRADITIONAL BANKS	
Online account opening	Implementing IDV technology in traditional banking for online account opening transforms the customer experience by enabling a swift, secure, and fully online process. Customers can upload a photo of their government-issued ID and take a selfie for biometric verification, significantly reducing the need for manual checks and in-person visits. This not only accelerates account creation from days to minutes but also enhances security by preventing identity theft and fraud through advanced verification layers. Furthermore, it ensures compliance with KYC and AML regulations, broadening access and inclusion by making banking services more accessible to individuals who might otherwise face barriers in visiting physical branches.
Mobile banking login	By leveraging biometric verification, such as facial recognition, IDV ensures that only the legitimate account holder can access their mobile banking app. This method replaces or supplements traditional passwords, which are often vulnerable to theft or forgetfulness, with a more secure and user-friendly alternative. The seamless and quick verification process not only fortifies the bank's defenses against unauthorized access and fraud but also enhances the customer experience by enabling a

	frictionless login that fits effortlessly into their daily routine.
High-risk transaction authentication	Having IDV technology can securely authenticate high-risk transactions by verifying the customer's identity through advanced biometric checks, such as facial recognition, ensuring the transaction is legitimate and reducing fraud and building customer trust.
Fraud prevention for online & mobile transactions	Having IDV technology can securely authenticate high-risk transactions by verifying the customer's identity through advanced biometric checks, such as facial recognition, ensuring the transaction is legitimate and reducing fraud and building customer trust.
Customer support authentication	IDV technology streamlines customer support authentication by using biometric verification to quickly and accurately confirm a customer's identity during support interactions. This enhances security and efficiency, reducing the risk of identity theft while providing a seamless and secure customer service experience.
ATM authentication	IDV enhances ATM authentication by employing biometrics, such as fingerprint or facial recognition, to verify the user's identity, ensuring that only the account holder can access their funds. This method increases security by reducing the reliance on easily compromised PINs and cards, effectively preventing unauthorized withdrawals and fraud.
In-branch identity verification	Implementing an IDV solution streamlines in-branch identity verification by using biometric data, such as facial recognition or fingerprint scanning, to quickly and accurately confirm a customer's identity. This reduces wait times, minimizes human error, and enhances security, providing a seamless and efficient experience for both customers and bank staff.
Employee access control	IDV secures employee access control by using biometric authentication, such as fingerprint or iris scans, to ensure that only authorized personnel can access sensitive areas and information. This enhances security protocols, reduces the risk of insider threats, and ensures compliance with regulatory standards for data protection.
CHALLENGER BANKS/FINTECH	
Onboarding process	IDV technology streamlines the onboarding process by using biometric verification and document authentication to quickly and securely verify a new customer's identity. This ensures regulatory compliance, reduces fraud, and provides a seamless, user-friendly experience that can be completed entirely online.
Mobile app login	IDV enhances mobile app login by employing biometric authentication, such as facial recognition or fingerprint

	scanning, to ensure secure and swift access for users. This approach not only bolsters security by preventing unauthorized access but also offers a seamless and convenient login experience, aligning with the digital-first nature of challenger banks.
Passwordless authentication	IDV enables passwordless authentication by utilizing biometrics, such as facial or fingerprint recognition, to verify user identities, eliminating the need for traditional passwords. This approach enhances security by reducing the risk of password-related breaches and provides a more convenient and frictionless user experience, aligning with the innovative ethos of challenger banks.
Continuous authentication for high-risk transactions	An IDV solution supports continuous authentication for high-risk transactions by re-verifying user identities through biometric data ensuring ongoing security throughout the transaction process. This proactive approach enhances fraud prevention measures and provides real-time monitoring to swiftly detect and respond to any suspicious activities, maintaining trust and security for customers.
Fraud detection & prevention	IDV technology plays a crucial role in fraud detection and prevention by analyzing user behavior and biometric data to flag suspicious activities in real-time, thereby mitigating risks and protecting customers' financial assets. This advanced capability enhances the bank's security framework, instilling confidence among customers and ensuring compliance with regulatory requirements.
Compliance with KYC (Know Your Customer) & AML (Anti-Money Laundering) regulations	An IDV solution in challenger banks streamlines compliance with KYC and AML regulations by quickly and accurately verifying customer identities using biometric and document verification, reducing fraud risk and ensuring regulatory adherence. This efficient verification process not only enhances security but also improves customer onboarding experiences and customer trust..
Secure digital signature for contracts and agreements	IDV enables challenger banks to offer secure digital signatures for contracts and agreements by ensuring the signer's identity through biometric authentication and real-time document verification. This enhances the integrity and legal enforceability of digital transactions, providing a seamless and trustworthy user experience.
Biometric-based payment authorization	IDV facilitates biometric-based payment authorization in challenger banks, allowing customers to securely confirm transactions using unique biometric data such as facial recognition. This not only enhances security by reducing fraud but also offers a convenient, swift, and user-friendly payment experience.

CREDIT UNIONS	
Member onboarding & identity verification	IDV technology streamlines member onboarding in credit unions by enabling instant, secure identity verification through digital channels, reducing the need for in-person visits and paperwork. This enhances member experience and operational efficiency, while ensuring compliance with regulatory requirements.
Secure online & mobile banking access	IDV technology provides secure online and mobile banking access for credit union members by verifying identities in real-time through biometric authentication and multi-factor authentication methods. This ensures that only authorized users can access their accounts, protecting against fraud and enhancing overall account security.
Contactless authentication for in-branch services	IDV enables contactless authentication for in-branch services at credit unions by using biometric identifiers, such as facial recognition or fingerprint scanning, to verify members' identities quickly and securely. This reduces physical contact, enhances safety, and speeds up service delivery, improving the overall member experience.
Fraud prevention for online & mobile transactions	IDV enhances fraud prevention for online and mobile transactions in credit unions by employing advanced algorithms and multi-factor authentication to detect and block suspicious activities. This protects members' accounts from unauthorized access and reduces financial losses due to fraud.
Member support authentication	IDV streamlines member support authentication in credit unions by using biometric and multi-factor authentication methods to verify members' identities quickly and securely during support interactions. This enhances the security of sensitive information while improving the efficiency and user experience of support services.
Secure loan application process	IDV technology secures the loan application process in credit unions by verifying applicants' identities through digital and biometric methods, ensuring that only legitimate applicants can proceed. This reduces the risk of identity theft and fraud, speeding up approvals and enhancing trust in the loan process.
Biometric authentication for call center services	An IDV solution facilitates biometric authentication for call center services in credit unions by allowing members to verify their identities using fingerprints or voice recognition, ensuring secure and efficient access to their accounts. This reduces the need for traditional security questions, speeding up the authentication process and enhancing overall member satisfaction.

Employee identity verification and access control	IDV enhances employee identity verification and access control in credit unions by utilizing biometric and multi-factor authentication to ensure that only authorized personnel can access sensitive systems and areas. This strengthens internal security, reduces the risk of unauthorized access, and ensures compliance with regulatory standards.
APPLICABLE TO ALL FINANCIAL INSTITUTIONS	
Two-factor authentication (2FA) or multi-factor authentication (MFA)	IDV technology in financial institutions enhances security for 2FA and MFA by verifying a user's identity through biometric data or government-issued IDs, reducing fraud and unauthorized access. This ensures that even if a password is compromised, the additional verification step protects sensitive financial information.
Password reset & account recovery	IDV streamlines password reset and account recovery processes in financial institutions by securely verifying user identities through biometric data or official documents, ensuring only legitimate users can regain access. This reduces the risk of fraud and enhances user experience by providing a swift and reliable method for account recovery.
Age verification for age-restricted products & services	IDV enables financial institutions to accurately verify the age of users through government-issued IDs, ensuring compliance with legal requirements for age-restricted products and services. This prevents underage individuals from accessing restricted offerings while streamlining the verification process for legitimate users.
Secure document signing & verification	IDV facilitates secure document signing and verification in financial institutions by confirming the signer's identity through biometric data or digital ID verification, ensuring the authenticity of the signatory. This enhances trust and legal compliance, reducing the risk of forgery and unauthorized transactions.
Remote onboarding & identity verification for new clients	An IDV solution streamlines remote onboarding and identity verification for new clients in financial institutions by using biometric data and government-issued IDs to authenticate identities quickly and securely. This enables clients to open accounts and access services without needing to visit a branch, improving customer experience and operational efficiency.
Continuous authentication for extended user sessions	IDV technology provides continuous authentication during extended user sessions in financial institutions by periodically verifying the user's identity through biometrics or behavioral analysis. This ensures ongoing security and reduces the risk of unauthorized access if a session is left unattended or hijacked.

Identity verification for third-party integrations & partnerships	An IDV solution ensures secure identity verification for third-party integrations and partnerships in financial institutions by validating the identities of external users and entities through robust biometric or document-based methods. This minimizes the risk of fraud and enhances trust, facilitating seamless and secure collaboration with external partners.
Biometric-based authentication for VIP or high-net-worth clients	IDV technology offers biometric-based authentication for VIP or high-net-worth clients in financial institutions, providing an extra layer of security through advanced methods such as fingerprint or facial recognition. This ensures that sensitive transactions and account access are protected with the highest level of security, catering to the unique needs of these high-value clients.

Building trust in financial services

In each of these scenarios, IDV technology emerges as a cornerstone for the credibility of financial services operations. Its role goes beyond mere identity confirmation; it safeguards the principles of efficiency, security, compliance, and trustworthiness in the financial sector. Put another way, financial institutions are investing in IDV solutions not merely as a technological tool, but as a means to ensure secure access to financial services, protect customers' assets, and maintain the integrity of the financial system.

As AI's role in evolving the digital landscape continues to grow, it is difficult to overstate the significance of the role IDV software will play in shaping the future of financial services. By responsibly harnessing the potential of this groundbreaking technology, financial institutions can enter a new era of efficiency, security, and customer trust, ultimately building a more inclusive and robust financial ecosystem for individuals and businesses around the world.

7. Legal & Regulatory Framework for IDV

A legal and regulatory framework provides guardrails for the financial services sector to conduct identity verification in a manner that is lawful, secure, and respectful of individuals' rights. It sets the rules of the game, builds trust, and promotes responsible and effective governance.

What follows are the essential aspects of the legal and regulatory framework governing identity validation.

Privacy laws & data protection

Enterprises must navigate a complex landscape of privacy laws when handling personal data for identity validation. This includes compliance with regulations such as the General Data Protection Regulation (GDPR) in the European Union.

In the United States, these include the Health Insurance Portability and Accountability Act (HIPAA) related to health information, or laws like the Fair Credit Reporting Act in the area of consumer financial privacy. At the state level, there are a combination of comprehensive consumer privacy laws, such as California Consumer Privacy Act. Then there are data specific laws, like the Illinois Biometric Information Privacy Act. Understanding these regulations is critical to safeguarding customer data and maintaining trust.

Artificial intelligence laws

In the area of AI, new laws are still emerging. The EU AI Act is a comprehensive, landmark piece of legislation with extraterritorial applicability like the GDPR. In the US, there are several states that have passed sector specific AI laws, such as Illinois and New York.

In May 2024, Colorado surprisingly emerged as an AI policy leader by enacting the US's first comprehensive AI-specific law. The act takes effect in February 2026, subject to passing through local state legislative passages. As an indicator of legislation that may follow in the US, the Colorado AI law will require organizations to implement AI transparency and risk mitigation measures.

Identity verification laws

Different regions and countries may have specific laws and regulations pertaining to identity verification for various purposes, including financial transactions, access to government services, and more. It is crucial for financial services organizations to stay informed about and comply with these laws to ensure the legitimacy of their identity validation processes.

AML/KYC

Financial services companies must comply with anti-money laundering (AML) and know your customer (KYC) regulations to prevent financial crimes, including money laundering and terrorist financing. Governing global authorities include the Sixth Anti-Money Laundering Directive (6AMLD) in the EU, the Bank Secrecy Act (BSA) and USA PATRIOT Act in the US, and the Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act) in Australia.

Regulations are largely risk-based, with regions requiring companies to apply specific customer identification programs that include best practices to verify the identity of customers.

Digital signature laws

In many jurisdictions, digital signatures carry legal weight, enabling individuals to sign documents electronically. Financial businesses need to understand the legal status and requirements surrounding digital signatures to implement secure and legally valid virtual identity validation methods.

Interoperability standards

Enterprises often collaborate with other entities, both domestically and internationally. Interoperability standards, such as those outlined by the World Wide Web Consortium (W3C) and the International Organization for Standardization (ISO), play a vital role in ensuring that identity validation systems can work seamlessly across different platforms and organizations.

Accessibility & inclusivity regulations

Accessibility and inclusivity regulations ensure that all citizens, including those with disabilities, can access different services. Laws such as the Americans with Disabilities Act (ADA) in the US and the W3C's WCAG Guidelines emphasize the need for digital services, including identity validation processes, to be accessible to all.

Non-regulatory influences

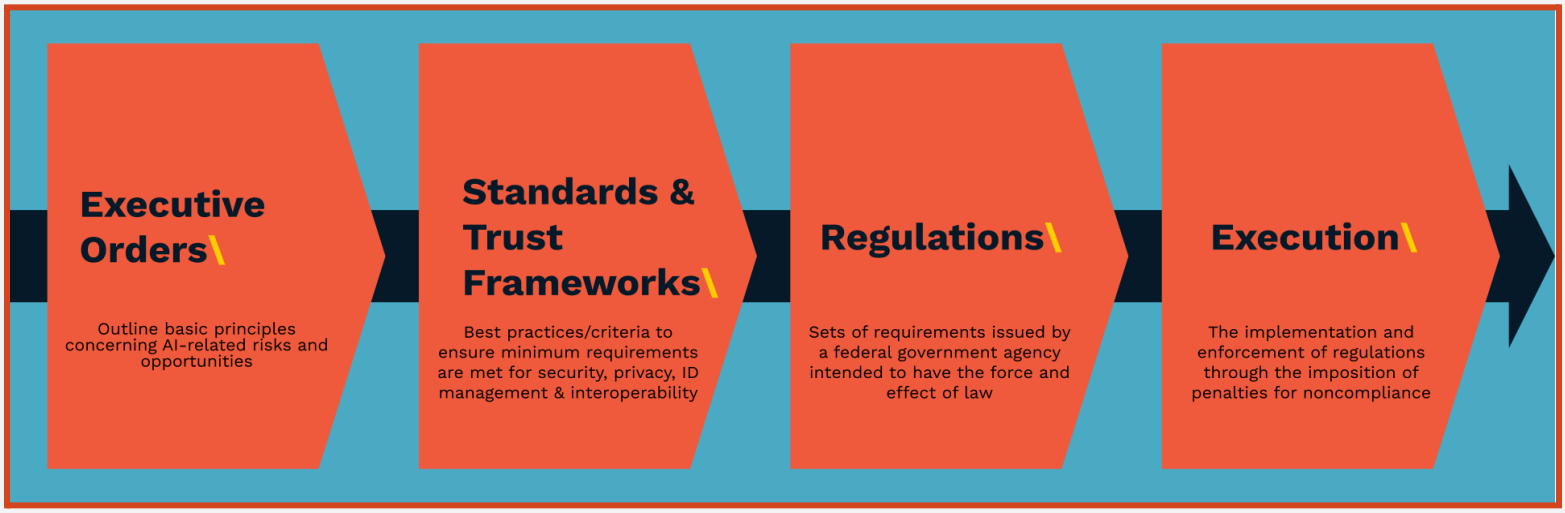
Outside of formally approved regulations, there are several other areas of strong influence on the policies and approaches required to be followed by corporations:

1. **Executive orders**: Issued by the senior executive leader, such as the US president or state governors, these directives are important in that they may mandate task forces to study cyber, privacy, AI and other controls and require government agencies to issue rules and guidelines that influence policy. Perhaps most noteworthy is the Biden administration's AI Executive Order issued in October 2023, for which rulemaking in the areas of auditing and assessments is very active as at the time of this guide release.
2. **Enforcement actions**: These types of actions highlight areas of priority for regulators and also interpret agency guidelines. In the enforcement arena in the US, the Federal Trade Commission (FTC) has been very active in enforcing

existing consumer protection laws. In the area of AI, a noteworthy action is FTC v. Rite Aid Corporation from December 2023, where the FTC outlined its expectations for companies in implementing responsible AI measures.

Both enforcement actions and executive orders are important to watch because they often send signals to legislators and regulators about the introduction of new laws and regulations.

3. **Litigation**: This is a very important active area particularly related to biometrics, AI and copyright issues. Litigation is important as it provides interpretation of laws.
4. **Non-government policies**: These policies, such as the G7 AI Code of Conduct, are also very influential and important to keep note of.

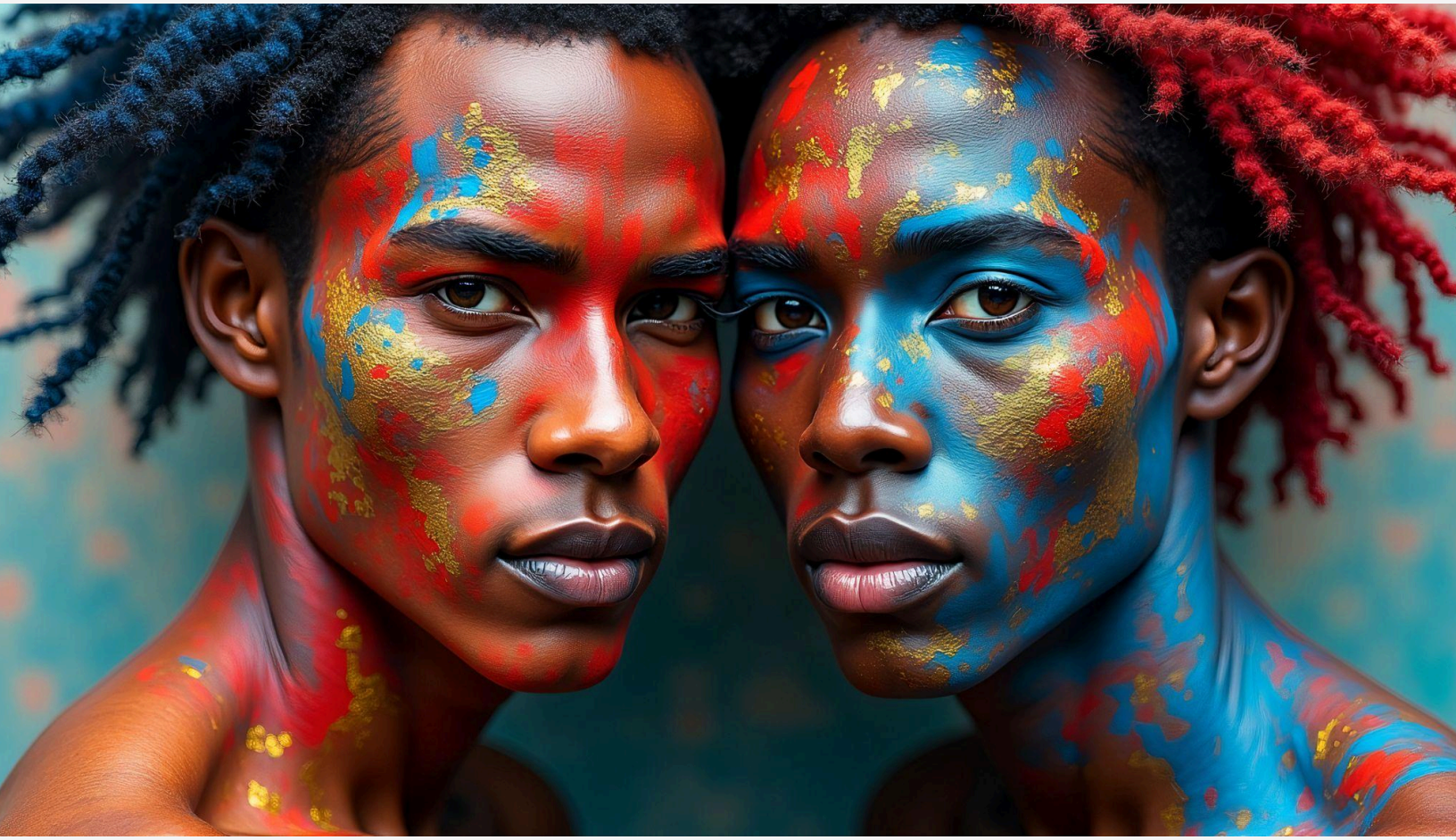


Ideas that carry weight
Principles alone cannot be enforced—they must be codified into regulations to truly compel compliance and enable oversight.

Navigating this legal, regulatory and policy landscape to develop identity verification systems that are not only secure but also compliant with the law will avoid legal repercussions and the erosion of customer trust.

The framework serves to promote compliance with laws, protection of data privacy, enhances security, builds trust, and

enables fair and equitable access to financial services while providing a structured approach to risk mitigation and accountability. It serves as the foundation for responsible and effective deployment of identity verification systems.



8. Best Practices

Adopting these best practices will help to ensure robust security, safeguard data privacy, and maintain compliance with evolving regulatory standards. To streamline these best practices, we categorize them into key areas:

Regulatory compliance

Stay current with an ever-changing landscape of data protection regulations. Adhere to legal frameworks such as GDPR, HIPAA, and government-specific guidelines. Additionally, ensure that identity verification solutions meet compliance requirements set by relevant regulatory authorities.

Ethical & fair practices

Maintain ethical considerations throughout the verification process. Implement policies and safeguards to ensure responsible and fair use of identity verification technology. To address concerns of bias in AI models, check if vendors use fair-sourced training data for AI models, promoting equity in verification processes.

Vendor due diligence

Vet identity verification vendors carefully. One crucial best practice is to check for certifications and standards that vendors adhere to. Ensure that vendors have undergone and maintained relevant certifications to guarantee the quality and security of their services. A thorough evaluation of vendor practices can be instrumental in securing the most reliable and ethical solutions for your identity verification needs. Refer to the Vendor Due Diligence Checklist for more information.

Security & data protection

Implement robust security measures to protect sensitive user data. Employ strong forms of multi-factor-authentication (MFA) to fortify verification processes, combining something the user knows (e.g. a password) with something they have (e.g. a mobile device) and something they are (e.g. a face). Furthermore, use encryption both for data in transit and at rest, ensuring that collected data is minimal, necessary, and well-protected.

User-centric design

Prioritize the user experience to enhance accessibility and efficiency. Design user-friendly interfaces with real-time feedback, facilitating a seamless journey through the verification process. Empower users with clear instructions and offer readily accessible support channels. Furthermore, educate staff on identity verification processes to ensure consistent, effective user assistance.

Best Practices in Virtual Identity Verification

Category	Best Practice
Regulatory Compliance	• Stay current with data protection regulations • Adhere to GDPR, HIPAA, and government guidelines
Ethical and Fair Practices	• Implement policies and safeguards for ethical use • Check if vendors use fair-sourced training data for AI models
Vendor Due Diligence	• Vet vendors based on certifications and standards
Security and Fraud Prevention	• Implement strong multi-factor-authentication (MFA) • Use encryption for data in transit and at rest. • Collect only necessary data and protect it
User-Centric Design	• Prioritize the user experience with clear instructions. • Design user-friendly interfaces with real-time feedback • Empower users with accessible support channels. • Train staff to ensure effective user assistance

By adopting these best practices in each of these five categories, government and public sector agencies can establish secure, compliant, and user-centric online identity verification processes. This not only safeguards user data but also fosters trust and confidence in government services, ultimately leading to more efficient and effective operations.

9. ROI: Return On Identity

Investing in a virtual biometric identity verification solution offers financial businesses a powerful opportunity to drive significant return on investment (ROI). These technologies obviously enhance security, but they also unlock a wide range of benefits that directly impact the bottom line.

This chapter will explore the various ways in which investing in virtual facial biometric IDV can optimize organizations' financial performance, positioning them for success in an increasingly competitive and technology-driven market.

Reducing fraud losses

Through the use of unique, individual physical characteristics, biometric IDV systems provide a level of security that traditional authentication methods (e.g. passwords or security questions) simply cannot match, as these can be easily compromised through phishing, social engineering, or data breaches.

The implementation of biometric authentication therefore allows financial businesses to drastically decrease the incidence of fraudulent activities, protecting both the organization and its customers from substantial financial losses. The result: millions of dollars saved annually and a direct positive impact on ROI.

Lowering operational costs

Automating manual identity verification processes with biometric IDV solutions streamlines operations, reducing the need for human intervention (e.g. manual reviews) and lowering associated costs. The increased operational efficiency achieved through these solutions translates into significant cost savings over time.

Improving customer acquisition & retention

Virtual biometric IDV solutions enable seamless, secure onboarding and authentication experiences that enhance customer satisfaction in the highly competitive financial services landscape.

Satisfied customers are more likely to remain loyal to the institution and recommend its services to others, leading to increased customer acquisition and retention rates. Higher customer retention and acquisition drive revenue growth and strengthen the company's market position.

Enhancing regulatory compliance

Financial organizations must adhere to stringent regulatory requirements, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations. Non-compliance with these requirements can result in hefty penalties and reputational damage.

Biometric IDV solutions help institutions meet these compliance standards by providing robust, auditable identity verification processes. Maintaining a strong reputation and avoiding costly penalties protects the company's bottom line and ensures long-term success.

Increasing efficiency & enabling new digital services

Biometric authentication streamlines customer interactions, reducing friction and enabling faster, more efficient transactions. The increased efficiency boosts productivity and allows financial businesses to serve more customers in less time.

Furthermore, secure biometric authentication paves the way for the introduction of new digital products and services, such as mobile banking and online lending. Expanding market reach and revenue streams through these innovations drives significant ROI.

Reducing support costs & protecting reputation

Password resets and associated customer support inquiries can be a significant drain on resources. Biometric authentication minimizes the need for these costly interactions, lowering helpdesk and IT support expenses.

Robust biometric security measures also help prevent data breaches and protect customer information. Safeguarding reputation and maintaining customer trust allows financial businesses to avoid the immense costs associated with reputational damage.

Competitive differentiation & cross-selling opportunities

Advanced biometric IDV solutions can set financial institutions apart from their competitors, attracting tech-savvy customers and establishing a reputation for innovation and security. This competitive differentiation can lead to increased market share and revenue growth.

The seamless, secure authentication experiences provided by biometric IDV solutions also facilitate cross-selling and upselling opportunities. Customers who feel their information is secure are more likely to engage with additional products and services, further contributing to the organization's bottom line.

Investing in a virtual facial biometric IDV solution offers a clear ROI for financial services. As the industry continues to evolve, companies that prioritize secure, seamless identity verification through biometric solutions will be best positioned to thrive in the future.

10. Future Trends

The field of identity verification is evolving very quickly, driven by advances in technology, shifting consumer preferences, and a regulatory landscape that's scrambling to keep up. In the coming years, we can expect to see IDV processes become faster, more convenient, and more secure as financial institutions look to leverage emerging technologies and adapt to new industry standards.

This chapter will explore some of the key trends and opportunities that are poised to reshape IDV in the financial sector.

Biometric authentication goes mainstream

Biometric authentication methods like facial recognition, fingerprint scanning, and voice identification have long held the promise of more secure and frictionless verification experiences.

As the underlying technologies mature and consumers grow more accepting of biometric security checks, we can expect to see biometrics become a mainstream component of IDV workflows. From selfie-based document verification to voice-based authentication in call centers, biometrics will enable faster, more reliable identity checks across a range of financial services contexts.

AI enables proactive fraud detection

Artificial intelligence and machine learning have immense potential to enhance the speed and accuracy of IDV processes. By analyzing massive datasets and identifying patterns that may elude human analysts, AI-powered systems can detect signs of fraud and identity theft more quickly and proactively flag high-risk individuals for additional screening.

As fraudsters grow more sophisticated in their methods, AI will become an indispensable tool for staying one step ahead and safeguarding customers' financial assets and personal data.

Decentralized ID solutions gain traction

Decentralized identity solutions built on blockchain technology offer a new paradigm for identity verification—one in which individuals have greater control over their personal data and can selectively disclose verified credentials as needed.

While decentralized identity remains in its early stages, a growing ecosystem of platforms and protocols is emerging to support self-sovereign identity models. Financial institutions that embrace decentralized identity early on will be well-positioned to offer their customers more secure, privacy-preserving verification options as adoption increases.

Mobile-first IDV becomes the norm

With the ubiquity of smartphones and the growing preference for mobile-first experiences, it's no surprise that identity verification is increasingly being conducted through mobile channels.

Mobile IDV solutions enable customers to complete verification workflows quickly and conveniently using the cameras, microphones, and other sensors built into their devices. Seamless integrations with mobile banking apps will make it easier than ever for financial institutions to embed verification touchpoints directly into the user experience.

Continuous authentication enhances security

Rather than treating identity verification as a one-time event, forward-thinking financial institutions are exploring ways to continuously authenticate users throughout their journey. Using behavioral biometrics, device fingerprinting, and other intelligent authentication signals, continuous authentication solutions can

detect potential fraud in real-time and prompt for step-up verification when risk levels change.

This adaptive, risk-based approach to authentication will enable financial institutions to deliver more secure experiences without creating undue friction.

Digital IDV expands globally

As more countries develop digital identity infrastructures and standards for digital IDs, the use cases for identity verification will continue to expand globally. From electronic passports to government-issued digital ID cards, digital credentials will play an increasingly important role in cross-border financial transactions and anti-money laundering efforts.

Financial institutions will need identity verification solutions that can work with a wide range of international electronic ID systems and adhere to country-specific regulations and standards.

User experience drives differentiation

In an era where customers expect fast, frictionless digital experiences, user experience will increasingly become a key differentiator for financial institutions. Identity verification workflows that feel clunky or time-consuming will frustrate customers and negatively impact conversions and retention.

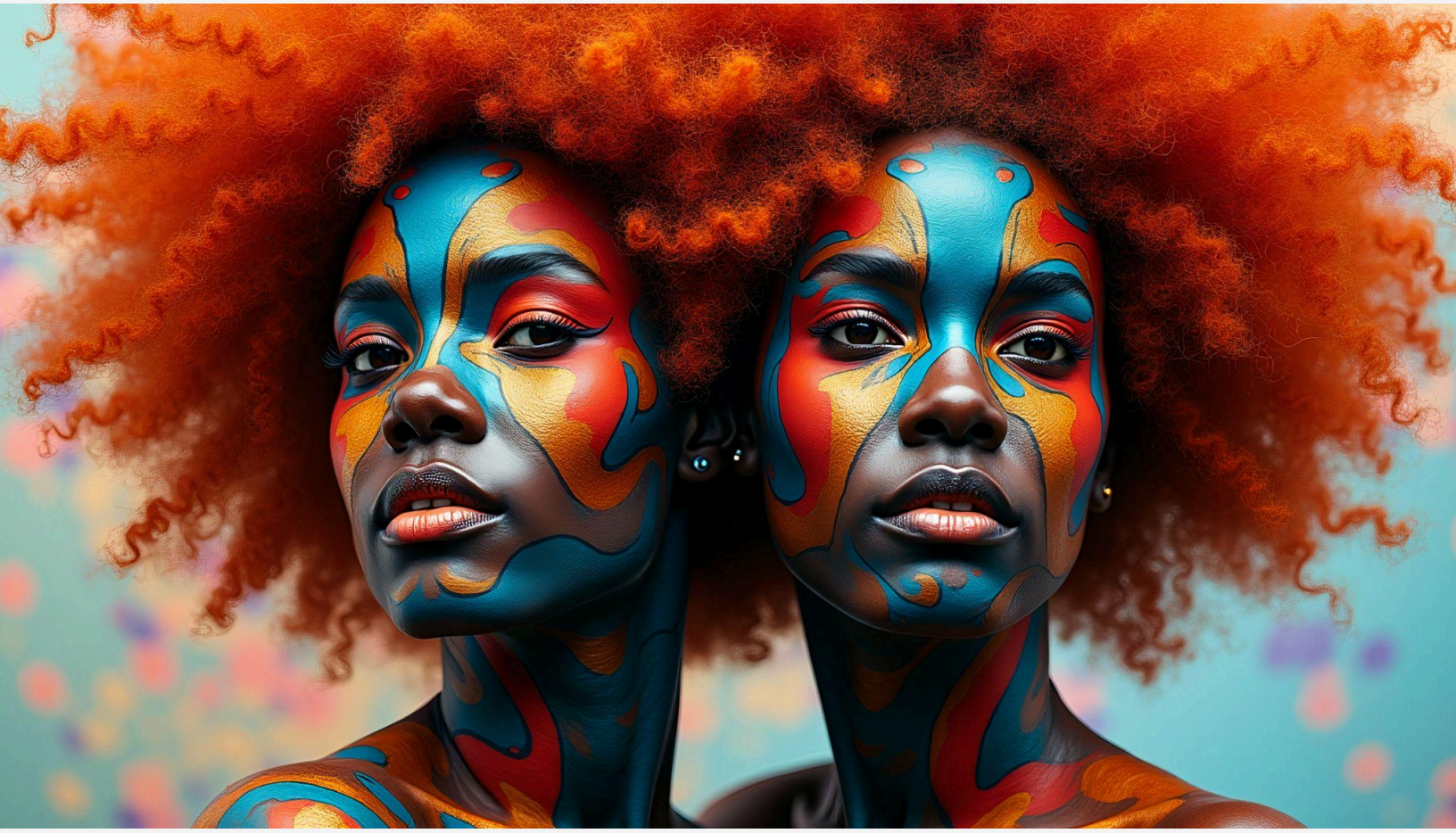
To stay competitive, financial institutions will need to invest in IDV solutions that balance security with user-friendly experiences. Intelligently designed user interfaces, clear messaging around why certain data is collected, and flexible options for completing verification steps will all be essential for delivering an optimal verification experience.

Keeping up with what's next

The future of identity verification in the financial sector is marked by both challenges and opportunities. As fraudsters grow more

sophisticated and regulators introduce new requirements, financial institutions will need to continually adapt their IDV processes to stay ahead.

At the same time, emerging technologies and shifting consumer preferences are opening up new possibilities for faster, more secure, and more user-friendly verification experiences. Financial institutions can build trust with their customers and thrive by staying attuned to these trends and investing in forward-looking IDV solutions.



11. Conclusion

Virtual identity verification is an indispensable tool enabling the financial sector to thrive in a world that's becoming more and more digital with each passing day. As explored throughout this paper, IDV solutions backed by artificial intelligence strengthen security, combat fraud, optimize processes, and facilitate digital transformation across financial services use cases.

To fully harness the potential of this technology, however, financial services businesses entities must prioritize privacy while eliminating bias and embracing inclusion. Through responsible development and deployment of IDV systems, the financial sector can enter an era of efficient, user-friendly services that engender trust among those they serve—but this requires selecting partners who are also committed to mitigating algorithmic bias via techniques like diverse data sourcing, regular audits, and transparent development practices.

Ultimately, offsite identity verification represents a pivotal innovation shaping the financial sector's digital future. Yet its full promise will only be realized through a shared commitment by governments, private enterprises, and end users alike to uphold principles of accessibility, security, privacy, and fairness.

By working together proactively, the immense possibilities of IDV can be channeled to benefit all members of society equitably. This vision will enable online identity solutions to strengthen financial sector operations today and for decades to come.

Appendix

States of data & data management

Organizations must navigate a delicate balance between using customer data for business purposes and respecting individuals' privacy rights—or else risk significant financial and reputational harm. Among the sundry items a business must take into account are obtaining informed consent for processing of biometrics, being transparent about data collection and usage practices, implementing robust security measures to protect customer data, and providing individuals with control over their own data.

Understanding the different states of data is crucial for maintaining its security and integrity. We can categorize data into three distinct states: data at rest, data in transit, and data in use. Each state represents a unique phase in the lifecycle of information, with its own set of considerations and risks. By understanding these states, companies can effectively implement measures to safeguard data throughout its journey.

Vendor Due Diligence Checklist

Questions to ask a provider about their handling of data at rest:

1. Does your platform allow us to set automated data deletion rules?
2. What is the shortest period that we can set?
3. How long is the data retained in your engines themselves? (Data is often held in engines separately to the main platform.)
4. What is your data deletion policy for Illinois residents, including any backups?
5. Can you prove that you do delete when you say you do?
6. Can we delete all biometric and photo data from the records you keep for us?

7. Is data held in backup, and for how long? (In order for an organization to recover data and the results of checks in the event of a severe incident, the organization will need to make copies of data into backup. Typically the data resides in backup for a set period, say 30 or 60 days. When you delete data from the main platform, the backup data will not usually be deleted. So you need to ask how long that backup retention period is. The risk of storing data in backup is much lower because the backup data cannot be accessed via the platform, which from a security perspective is normally the weakest link, but you still need to ask the questions.)
8. Is data held in your training database? If so, for how long?

Questions to ask a provider about their handling of data in transit:

1. In which jurisdiction will the data of my end users be hosted?
2. Can we select different jurisdictions for data hosting depending on where the data originated?
3. At any point in the IDV process, is any data transferred from the UK or the EU into the US?
4. If yes to Q3, what is the lawful mechanism the transfer is made under?
5. Is my end user data used in any fraud signal sharing database? If so, please share your Data Protection Impact assessment so we can understand the legality of this processing.

Questions to ask a provider about their handling of data in use:

1. Please show me your consent screen and show me your legal advice that it complies with BIPA and CUBI (the Capture or Use of Biometric Identifier Act, Texas' less scary version).
2. Where can I read your public "biometric processing statement"?

3. Do you use the data of Illinois residents in any form of training?
4. Can you send me your Data Protection Impact Assessment (DPIA) covering the service you are selling to me?
5. How have you trained your algorithms?
6. Will you be reusing personal data from our end users to train your algorithms, and if so, what is your lawful processing ground?
7. From where do you source your training data?
8. How have you, or the source of your data, collected express consent from the data subjects?
9. Can you prove to us that you have that consent?
10. How can a person withdraw consent if they later change their mind?

Certifications

The various certifications from Table 1 explained:

Certification Standards and Governing Bodies

Certification Type	Scope
NIST: National Institute of Standards and Technology (U.S. Dept. of Commerce)	
Basic certification	• NIST SP 800-171: Cybersecurity standards for protecting controlled unclassified information
Advanced certification	• NIST SP 800-53: Cybersecurity framework that provides guidelines for federal information systems • NIST SP-800 63 IAL 2: Cybersecurity standard that provides identity assurance in digital and online transactions
iBeta/BixeLab against ISO 30107-3 (Biometric testing lab)	
Basic certification	• Liveness PAD Level 1: Basic presentation attack detection for biometrics
Advanced certification	• Liveness PAD Level 2: Enhanced presentation attack detection for biometrics • Liveness (bias testing): Testing for bias in biometric systems
Government entities	
Basic certification	• CPRA: California Privacy Rights Act for data privacy rights • GDPR: EU's General Data Protection Regulation for data privacy rights •
Advanced certification	• TDIF L3: The Australian Government's Trusted Digital Identity Framework • DIATF: The UK Government's Digital Identity Authentication Trust Framework •

ISO (International Organization for Standardization)

Basic certification	• ISO 9001: Quality management systems • ISO 22301: Business continuity management • ISO 29100: Privacy framework
Advanced certification	• ISO 27001: Information security management • ISO 27017: Cloud security • ISO 27018: Cloud privacy • ISO 27701: Privacy information management • ISO 19795: Biometric performance testing • ISO 30107-3: Biometric presentation attack detection

AICPA SOC (System and Organization Controls)

Basic certification	• SOC 1: Financial controls audit
Advanced certification	• SOC 2: Security, availability, processing integrity, confidentiality and privacy controls audit

AICPA SOC (System and Organization Controls)

Certifications	Scope
Basic certification	• SOC 1: Financial controls audit
Advanced certification	• SOC 2: Security, availability, processing integrity, confidentiality and privacy controls audit

About the authors

Terry Brenner *is Head of Legal, Risk & Compliance, Americas, for IDVerse. Previously he has served in executive office and general counsel roles, in both start-up and mature businesses, across a range of diverse industry sectors. His focus at IDVerse is to lay the path for the successful integration of IDVerse's identity verification technology into the Americas market, heeding to the sensitivities around data and privacy protection.*

Peter Violaris *is Global DPO and Head of Legal EMEA and APAC for IDVerse. Peter is a commercial technology lawyer qualified in England and New South Wales with a particular focus on biometrics, privacy, and AI learning. Peter has been in the identity space for 6 years and before that worked for London law firms.*

Paul Warren-Tape *is IDVerse's SVP Risk and Compliance. He has over 20 years of global experience in governance, operational risk, privacy, and compliance, spending the last 10 years in pivotal roles within the Australian financial services industry. Paul is passionate about helping organizations solve complex problems and drive innovation through encouraging new ideas and approaches, whilst meeting their legislative requirements.*

About IDVerse

IDVerse is the leading automated identity verification platform to onboard and re-authenticate trusted users at scale.

What sets us apart? Our commitment to Zero Bias AI™ means that we are pioneering the use of machine learning to protect against discrimination on the basis of ethnicity, age, and gender. We build software capable of authenticating tens of thousands of ID document types and verifying the liveness of billions of real people without manual human intervention—all underpinned by generative AI that achieves maximum inclusion and fairness.

IDVerse can recognize over 16,000 ID types in 142 languages from more than 220 countries and territories. The world's leading companies like Amex, HSBC, and Hertz trust us to help their users prove their identity in seconds.

The IDVerse solution has been tested and certified to meet the most stringent standards in the industry, including NIST, ISO, iBeta, and algorithmic Zero Bias AI™ specifications.

Want to learn more? Book a demo today, or get in touch with us at hello@idverse.com.