

MARCH 2024

# IDverse™

## THE PARTNERS GUIDE TO IDVERSE

**IDENTITY VERIFICATION  
INTEGRATE IN DAYS,  
ROI IN WEEKS**



**DEEPPFAKE DEFENDER**

**GENERATIVE AI & THE  
NEXT ERA OF FRAUD TECH**

# Table of Contents

|  |           |
|--|-----------|
| <b>Table of Contents.....</b>                        | <b>1</b>  |
| <b>Introduction.....</b>                             | <b>3</b>  |
| <b>1. A New Era of Tech &amp; Fraud Trends.....</b>  | <b>5</b>  |
| New threats posed by AI.....                         | 5         |
| How gen AI is used to fight deepfake fraud.....      | 7         |
| Facial biometrics are the way forward.....           | 7         |
| The role of AI in IDV.....                           | 8         |
| Bias in AI.....                                      | 9         |
| AI ethics & data nutrition labels.....               | 10        |
| <b>2. Meet IDVerse.....</b>                          | <b>13</b> |
| A brief history of our company.....                  | 13        |
| Dedication to eliminating bias.....                  | 14        |
| The solution.....                                    | 17        |
| IDV certifications.....                              | 19        |
| <b>3. Responding to Customer Demand.....</b>         | <b>21</b> |
| Enhancing customer experience.....                   | 21        |
| Adapting to the evolving nature of ID documents..... | 21        |
| Removing bias from decision making.....              | 22        |
| Multi-factor and decentralized identity.....         | 23        |
| New territories, new customer demands.....           | 23        |
| Leveraging expertise to stay ahead of trends.....    | 23        |
| Driving accuracy rates.....                          | 24        |
| <b>4. Ease of Being a Partner.....</b>               | <b>26</b> |
| Integrate today, revenue tomorrow.....               | 26        |
| Fewer vendors, more efficiency.....                  | 27        |
| Scaling beyond bottlenecks.....                      | 28        |
| Easing the technical lift.....                       | 29        |
| Integrating brand continuity.....                    | 30        |
| Several ways to be a partner.....                    | 30        |
| <b>5: Growing Together.....</b>                      | <b>33</b> |
| Complementary addition to your product suite.....    | 33        |
| Fast time to revenue.....                            | 33        |
| Flexible solution models.....                        | 33        |
| Enable globalization.....                            | 34        |
| Access to subject matter experts.....                | 34        |

**6. Our Belief in Partnerships..... 36**

    True partnership is a two-way street.....36

    Alignment of strategic goals..... 36

    Success through purposefulness..... 37

    Unite against bias and fraud..... 37

**Appendix..... 39**

    Certifications..... 39

        NIST: National Institute of Standards and Technology  
        (U.S. Dept. of Commerce)..... 39

        iBeta/BixeLab against ISO 30107-3 (Biometric testing lab)..... 39

        Government entities..... 39

        ISO (International Organization for Standardization)..... 40

        AICPA SOC (System and Organization Controls)..... 40





# Introduction



This guide is tailored for prospective partners and professionals interested in unlocking growth opportunities through strategic collaboration with IDVerse. It serves as a comprehensive guide, offering insights into the benefits and possibilities that come with partnering with the leading identity verification (IDV) solution provider.

Identity verification is rapidly evolving, driven by the increasing demand for seamless and secure digital experiences. IDVerse is a trusted partner helping businesses and organizations to navigate this dynamic environment. Together, we can drive innovation, success and profitability.

Identity verification trends are reshaping the way organizations approach security and user experience. From the widespread adoption of biometric authentication to the proliferation of mobile-friendly IDV solutions, the possibilities are far-reaching and transformative.

The convergence of remote, digital, and fully automated IDV—spurred by the COVID-19 pandemic where manual, human reviewers could not access their terminals—accelerated the urgency for reliable and efficient verification processes. Privacy-enhancing technologies, cross-industry collaboration, and adherence to international standards are key pillars shaping the future of identity verification.

Accessibility and inclusivity in IDV processes are also gaining prominence, reflecting a heightened awareness and commitment to ensuring equal access and participation for all individuals. Moreover, the emergence of digital identity wallets and the integration of open banking concepts are redefining how businesses and consumers interact with identity verification solutions.



**In the following chapters, we delve into the significance of trusted identity solutions and IDVerse's commitment to building partnership capabilities:**

1. A New Era of Fraud & Tech Trends
2. Meet IDVerse
3. Responding to Customer Demand
4. Ease of Being a Partner
5. Growing Together
6. Our Belief in Partnerships



# 1. A New Era of Tech & Fraud Trends

Generative AI—a type of artificial intelligence technology through which content such as text, images, audio, and video can be produced via written prompts—has rapidly become a global change maker.

Even outside of the tech industry, you’d be hard pressed to find someone who hasn’t heard of ChatGPT, Midjourney, DALL-E, or any of the dozens of other generative AI tools that have been released to the public at low (or no) cost.

The outputs of these systems can be stunningly convincing and lifelike, or wildly imaginative and surreal. Midjourney, for instance, can generate photorealistic images of people, objects, or scenes that never actually existed which can then be animated with tools like Runway. Meanwhile, ChatGPT produces human-like writing on virtually any topic with coherence and nuance.

There’s no question that generative AI represents a massive leap forward in Artificial Intelligence’s (AI) creative capabilities. These models can increase productivity in areas like content creation, graphic design, and more. However, in the wrong hands, they also enable sophisticated identity fraud.

## New threats posed by AI

The emergence of synthetic media, more commonly known as deepfakes, has introduced new challenges. Deepfakes are powered by sophisticated AI algorithms and enable the creation of highly realistic, manipulated video, image, and audio hoaxes that can convincingly impersonate individuals.

They often work by transforming existing content where one person is swapped for another, and they can be incredibly hard to detect with the human eye.

Deepfakes are challenging to detect for several reasons:

- **Advancements in technology:** Deepfake generation techniques continue to improve, with sophisticated algorithms and neural networks that can create ever more highly realistic forgeries.

25% of all fraudulent documents we're stopping now is synthetic media, that is, created by generative AI.

PAUL WARREN-TAPE, IDVERSE

- **Availability of training data:** Deepfake algorithms require large amounts of data to train effectively. With the abundance of publicly available images and videos online, perpetrators have ample material to create convincing forgeries.
- **Speed and accessibility:** Deepfake creation tools are becoming more accessible and user-friendly, allowing individuals with limited technical expertise to produce convincing forgeries quickly.
- **Adversarial tactics:** Perpetrators actively work to evade detection by employing techniques such as adversarial training, which involves training deepfake models to specifically counter detection algorithms.

Identity fraud facilitated by deepfakes has therefore become a massive concern for organizations around the world.





## How gen AI is used to fight deepfake fraud

While it's clear that generative models enable the latest fraud innovations, the same technology also powers the solutions. AI-driven identity verification leverages the same types of science used by threat actors, turning it against them.

For instance, software computer models that are capable of detecting synthetic media are trained, tuned, and de-biased with AI-generated photographs, videos, and documents. In a process using what is called generative adversarial networks (GANs), two components are employed: a generator and a discriminator. The generator creates synthetic deepfakes resembling genuine content, while the discriminator learns to differentiate between real and fake data.

Through iterative training, both components improve: the generator produces more convincing forgeries, and the discriminator becomes better at detecting them. This approach enhances the detection of deepfakes by leveraging the insights gained from creating realistic synthetic data or “goodfakes.”

Additionally, a key difference between a deepfake and a real human is “signs of life” or “proof of humanity.” Advanced IDV solutions using computer vision can recognize human liveness traits, such as image depth and a heartbeat through skin color change, by incorporating NIST-accredited biometric analysis into their technology.

## Facial biometrics are the way forward

Facial analysis represents the most secure and intuitive form of identity verification biometrics. The human face contains the richest blend of uniqueness and permanence. Even identical twins have distinguishable facial differences.

Additionally, face recognition is an innate ability in humans, and even babies demonstrate the capacity to recognize familiar faces, such as those of their parents, shortly after birth.

This is because the human brain is highly specialized in processing facial information. Specialized regions of the brain, such as the fusiform face area (FFA), are dedicated to facial recognition and play a crucial role in distinguishing between familiar and unfamiliar faces.

Unlike passwords, advanced facial biometrics cannot be lost, forgotten, stolen, or easily faked. Face biometrics provide a convenient and user-friendly authentication method, eliminating the need to remember and manage complex passwords while offering quick access to devices or systems.

Finally, photographs from government ID documents or databases provide reliable, third-party facial reference data. Verification solutions compare live selfies to official ID pictures, confirming that the user showing the ID is the legitimate owner.

This alignment with authoritative databases of faces makes facial biometrics reliable compared to others like voice, fingerprint, or behavioral that do not have ubiquitous libraries of reference data.

## **The role of AI in IDV**

As generative AI technology gains unprecedented sophistication, legacy security practices no longer provide adequate fraud protection. As discussed above, passwords are static, hackable data points ill-equipped to mitigate evolving threats—which have no doubt been leaked in the numerous past breaches.

Fighting back requires equipping IDV with new, powerful, and effectively trained generative AI and security form factors.

AI-powered computer vision analyzes identification documents and selfie captures with unrivaled speed and precision. By scrutinizing visual imagery via pattern recognition and geometrical facial mapping, AI solutions immediately flag hundreds of fraud indicators while resisting manipulation tricks that could dupe human reviewers.



## Bias in AI

Bias in AI refers to the unfair or discriminatory treatment of individuals or groups based on their ethnicity, age, gender, or related factors, perpetuated by AI systems. In a real-world setting, this bias can manifest in various forms, such as unfair decision-making in hiring processes, biased criminal risk assessments, and discriminatory content recommendations on social media platforms.

Let's explore the three primary sources of bias when it comes to artificial intelligence:

- **Data bias:** One of the most significant sources of racial bias in AI is biased training data. AI systems learn from inputted data, and if this data reflects societal prejudices or disparities, the AI is likely to replicate these biases. For instance, if a facial recognition system is trained on a dataset that underrepresents certain racial groups, it may perform poorly for those groups.
- **Algorithmic bias:** The algorithms used in AI systems can also introduce bias. For example, a predictive policing algorithm may disproportionately target certain neighborhoods, leading to racial profiling. Biased algorithms can thus further exacerbate existing inequalities.
- **Human bias:** Racial bias can also creep into AI through the humans who design and develop these systems. Biased decision-making during the development process, whether intentional or unintentional, can influence an AI's behavior.

As mentioned above, racial bias in AI can have far-reaching consequences including:

- **Reinforcing discrimination:** Biased AI systems can perpetuate existing racial discrimination and disparities by making decisions that negatively impact marginalized groups.



- **Privacy violations:** Biased facial recognition systems can lead to privacy violations, as individuals from certain racial backgrounds may be disproportionately tracked and surveilled without their consent.
- **Legal and ethical challenges:** Organizations deploying biased AI systems may face legal and ethical challenges, potentially leading to lawsuits, public backlash, reputational damage, and major revenue loss.

## AI ethics & data nutrition labels

As generative models achieve unparalleled realism, ethical considerations around responsible data usage grow increasingly pertinent. As described above, the training data used to develop generative systems introduces risks of perpetuating or exacerbating societal biases if not properly audited and governed.

In response, the concept of mandating data transparency has gained significant traction. Data “nutrition labels,” like ingredient



The image shows a man in a dark blue suit and yellow striped tie holding a blue box of 'AI POPS' cereal. The box features a bowl of yellow cereal and the text 'AI POPS'. A large blue arrow points from the box to a 'Nutrition Facts' label on the right.

| Nutrition Facts  |                    |
|--|--------------------|
| Serving size   | 1 piece of content |
| Fair Representation  |                    |
| Video Length   | 0:30               |
| % Daily Value*   |                    |
| Total Certifications   | 14                 |
| <div> <div>NIST 2 certs</div> <div>ISO 9 certs</div> <div>SOC 2 certs</div> <div>iBeta/BixeLab 1 cert</div> </div> |                    |
| Synthetic Training Data  | 100%               |
| Bias   | 0%                 |
| Watermarked  | Yes                |
| Fair Representation  | Yes                |
| Consent Yes  |                    |
| Includes Informed Consent  |                    |
| Overall Compliance   | 100%               |

listings for food products, would disclose full details on a dataset’s origins and composition.

Data nutrition labels should disclose:

- **Demographic distribution across gender, ethnicity, age, etc.**
- **Geographic representativeness**
- **Data collection methodology and consent protocols**
- **Results of bias testing audits**

For identity solutions leveraging generative AI, upfront transparency around training data characteristics enables more informed selections while catalyzing continual improvements in ethical data sourcing.

Substantial labeling requirements would preclude usage of datasets containing personally identifiable information without explicit opt-in consent. This is becoming more urgent for private sector businesses to address as governments begin to scrutinize and regulate AI privacy rights.

Generative models can produce endless variations of images, video, and text which encompass significantly broader ranges of representation compared to finite authentic datasets.



**Midjourney Prompt:** a photo realistic image of a turkish man in his 20s. in the format of a passport photo. Use a Sony α7 III camera with a 85mm lens at F 1.2 aperture setting to blur the background and isolate the subjects in front of a solid color background --v 6.0

To summarize, thoughtfully crafted synthetic data feeds algorithms the optimal “nourishment” for reaching their full potential while upholding ethics by avoiding direct usage of real people and personal user data.

As facial recognition technology continues to evolve, ethical considerations must remain at the forefront of businesses, governments and consumers alike. Ethical procurement of data ensures that this technology is used responsibly, respects individual rights, and remains an asset to humanity rather than a threat to privacy and civil liberties.

Prioritizing these things is not just a corporate responsibility; it's a societal imperative in an age where facial recognition touches so many aspects of our lives.



## 2. 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.

Under one minute. Customers previously waited up to three days for a manual review, now decreased to seconds.

**NICK JONES, HEAD OF CUSTOMER FULFILMENT, ADMIRAL MONEY**

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.

So Dan and Matt 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.

## Dedication to eliminating bias

At IDVerse, we strongly believe that AI-based identity verification companies must encode inclusivity into the algorithms that power their products. This helps to ensure that everyone, everywhere gets an equitable onboarding and authentication experience.

IDVerse is the only vendor who could accurately recognise people of different ethnicities and do liveness verification. I've had my own experiences of not being recognised by technology, and the ability to do this is critical to the business we are building.

**NINA MOHANTY, CO-FOUNDER, BLOOM MONEY**

Bias can manifest in a myriad of ways. For instance, a seemingly innocuous prompt such as "show me faces of successful business owners" on a typical image-generative AI platform like Midjourney can disproportionately favor Western, white, male faces, neglecting the fact that the vast majority—more than 75%—of the world's population lives in Asia and Africa.

AI programs often reinforce stereotypes because human engineering teams have inherent biases that get encoded into the algorithms. As leaders of technology, we therefore have found ourselves at the crossroads of innovation and responsibility. Our creations—the software solutions we engineer—can either exacerbate societal biases or serve as a force for positive change; the choice is ours to make.

IDVerse has anchored the principle of inclusivity into our software development process by developing the Code Zero Bias Oath. This credo is inspired by the enduring principles of the Hippocratic Oath, but tailored to the unique challenges and opportunities of our field. It embodies our collective 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.*

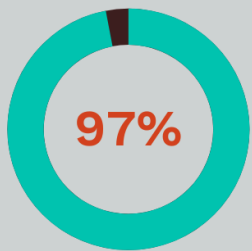
*By taking this **Code Zero Bias Oath**, software engineers demonstrate their dedication to ethical software development, with a focus on reducing algorithmic bias and promoting fairness, transparency, and accountability.*

## The solution

IDVerse is an end-to-end IDV solution that has the following capabilities:

- **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 & credit bureau databases—all in real time. This capability allows our customers to meet compliance obligations with either a simple API integration.

## Unrivalled accuracy & performance



of acceptance/  
rejection decisions  
provided in  
a minute or less



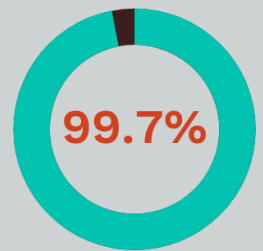
document fraud  
assessment  
accuracy



liveness video  
fraud assessment  
accuracy



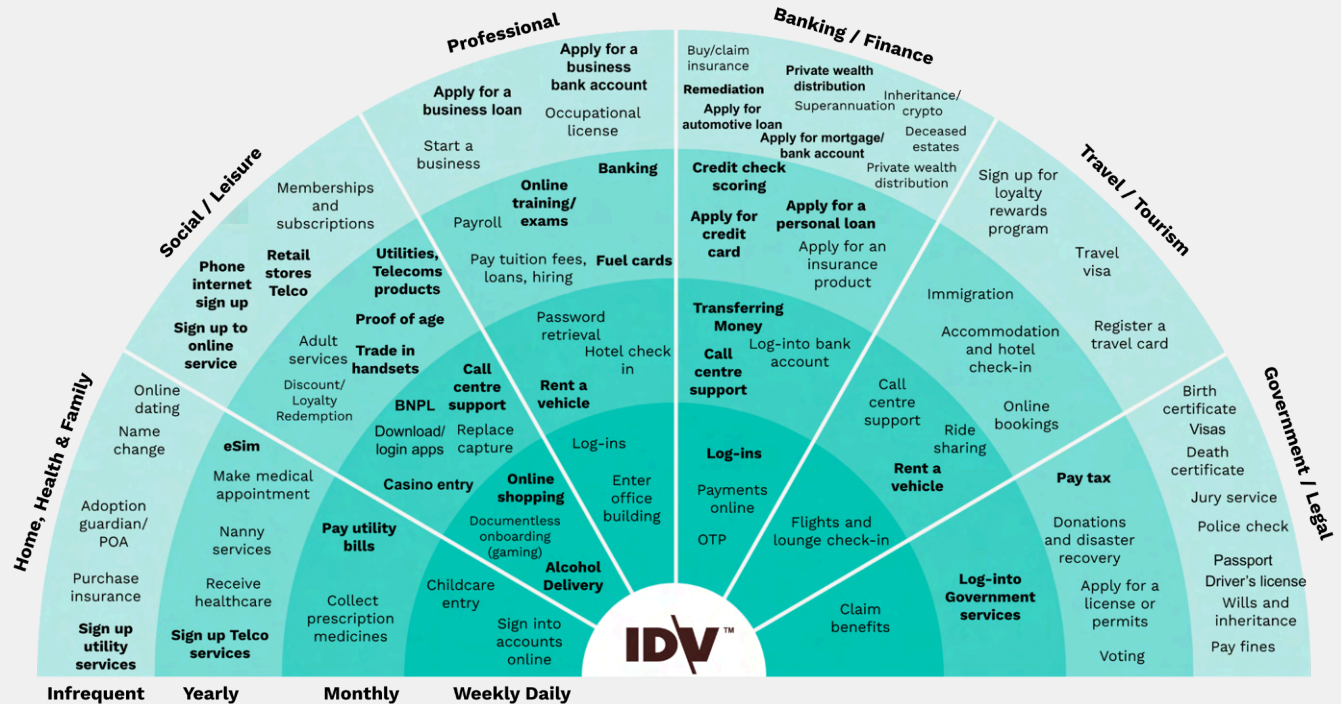
face-matching  
accuracy



of languages  
on printed ID  
documents can be  
read and extracted

- **Reauthentication:** 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**: An additional layer of fraud detection signals to identify recurring fraudsters or identity theft velocity attacks.
- **Proof Of Address**: Scan any printed document to extract the address and other key details.



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



## IDV 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.

| Certification body                                   | Basic certifications           | Advanced certifications  |
|--|--------------------------------|--|
| NIST   | NIST SP 800-171                | NIST SP 800-53, NIST 800-63 IAL2                                   |
| iBeta/BixelLab against ISO 30107-3                   | Liveness PAD Level 1           | Liveness PAD Level 2, Level B Bias testing                         |
| Government entities                                  | CPRA, GDPR                     | TDIF L3 (Australia), DIATF (UK), DocAuth                           |
| 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 (SOC)  | SOC 1                          | SOC 2  |

**Table 1.** See appendix for full explanation of certifications.



### 3. Responding to Customer Demand



Onboarding platforms find themselves at a crossroads where upgrading from manual identity verification vendors to fully automated solutions. Let's take a look at the factors that underscore the necessity of this upgrade and the opportunities it can generate.

#### Enhancing customer experience

A good customer experience is central to every successful user onboarding journey. Manual IDV processes often entail cumbersome procedures being placed on the user to submit information and prolonged waiting times for verification.

Such friction points not only deter potential customers but also impede the reauthentication of existing ones.

Leading IDV vendors should provide a rigorously tested user flow that gives a streamlined and intuitive experience, and allows partner platforms to significantly enhance customer satisfaction and retention rates.

#### Adapting to the evolving nature of ID documents

While the majority of people still hold physical ID documents, there are an increasing number of jurisdictions developing digital ID formats, as seen in Australia and the US. Just as payments have been disrupted by Apple Pay and Google Pay, the way in which users prove their identity is starting to embark on a similar journey.

Digital IDs and wallets are starting to be approved and enter circulation which provides a new challenge for identity verification vendors to accept a completely new format of identity with an even greater focus on instant user experience.



The ubiquity of digital IDs will first require standardization, followed by relying party and end-user adoption. This is evidenced by the release in 2021 of ISO 18013-5, which set the standard for mobile driving licenses (mDLs) for in-person scenarios (for example, presenting to an officer at airport security.)

Several States in the US followed this release by launching their version of mDL for the in-person use case. IDVerse is working with some of these States to advise on tools and approaches to increase adoption of their in-person mDLs.

Looking ahead, the future-state of mDLs will be around remote presentation by an end user of his/her mDL. ISO standards for this use case are expected to be released in April 2024 in a version 1 draft of ISO 18013-7. Here too IDVerse is engaged with numerous government, industry representative organizations and standards bodies to improve underlying standards, interoperability among different mDL standards (i.e. OpenID for Verifiable Presentations and Web3), and positive customer UX.

Despite the advance of remote mDLs to analyze digital IDs, accurate and zero bias assessment of user liveness through facial biometrics remains a key authentication point to tie the user to the digital document.

## **Removing bias from decision making**

Manual verification methods are inherently susceptible to human biases, whether conscious or unconscious, which can influence the assessment of identity documents and verification outcomes. This bias can manifest in various forms, including racial profiling, socioeconomic discrimination, and gender bias.

As mentioned previously, advanced machine learning algorithms can be trained on synthetic datasets to recognize and mitigate potential biases, ensuring fair and equitable outcomes for all users.

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**

### **Multi-factor and 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.

### **New territories, new customer demands**

With technological advancements continuing to penetrate previously underserved markets, there is a growing need for reliable identity solutions that can cater to diverse populations across the globe.

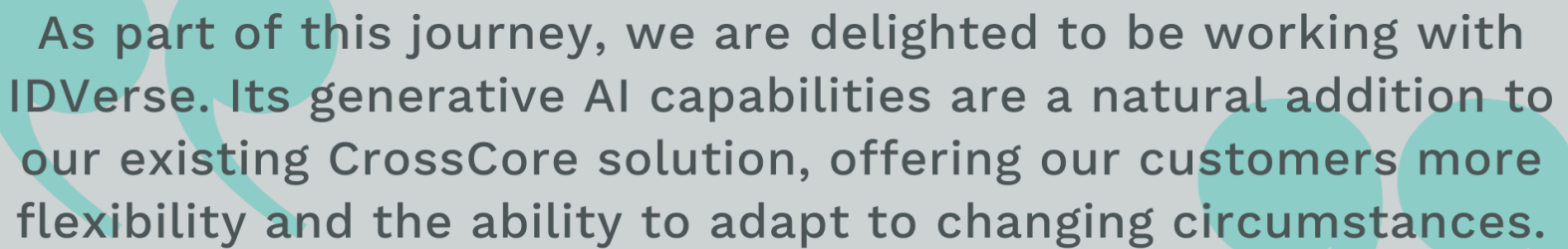
Upgrading to a fully automated IDV solution presents platforms with a significant opportunity to increase market share and revenues. Businesses operating in sectors such as cryptocurrencies, gig economies, and mobility are increasingly

relying on IDV services to facilitate secure transactions and comply with new regulatory requirements.

Scalability is another large factor. Fully automated systems allow partner platforms to optimize operational efficiency and reduce overhead costs associated with manual verification processes. Such solutions accelerate the onboarding process for new customers around the world, allowing platforms to grow their user bases at an exponentially faster rate.

### **Leveraging expertise to stay ahead of trends**

Working with external IDV experts allows partners to harness their specialized knowledge and experience in developing and implementing cutting-edge verification solutions. Platforms may lack the resources or expertise to build such sophisticated systems in-house, and attempting to do so could divert valuable time and resources away from their core business objectives.



As part of this journey, we are delighted to be working with IDVerse. Its generative AI capabilities are a natural addition to our existing CrossCore solution, offering our customers more flexibility and the ability to adapt to changing circumstances.

**EDUARDO CASTRO, MANAGING DIRECTOR ID&F, EXPERIAN UK&I**

External IDV solutions providers are dedicated to staying abreast of emerging trends, regulatory changes, and evolving fraud tactics. They continuously update their algorithms and processes to adapt to new challenges, ensuring that partner platforms remain at the forefront of identity verification best practices.

Investing in best-in-breed identity verification solutions is not just a strategic advantage but a business imperative for partner platforms seeking sustainable growth and success.

### Driving accuracy rates

Inaccurate verification results can lead to false positives or false negatives, creating friction in the user journey and undermining trust in the platform's security measures. Such imprecise outcomes can cause downstream operational issues that can consume valuable time and resources to resolve.

Fully automated solutions detect fraudulent or tampered documents, flag suspicious activities, and verify the authenticity of user identities with far greater reliability than manual methods. In improving the accuracy of the verification process, partner platforms mitigate the risk of fraud, enhance regulatory compliance, and safeguard sensitive consumer data more effectively.

A platform flagged an error with a Nigerian document on a Tuesday. We were able to retrain the system in 24 hours and update the solution. Our responsiveness is key to helping our partners succeed.

**LLOYD REEVE, IDVERSE**

In the long run, investing in a fully automated IDV solution helps you to answer the call of customer needs while minimizing operational overhead, mitigating risks, and driving sustainable growth for the partner platform.



## 4. Ease of Being a Partner

We like to enable and activate our partners. That's why we start with a clear launch plan to ensure that we get our working relationship heading in the right direction from day one.

We've wired on partners on a Friday and they were making revenue through us on Monday.

LIBBY ROBINSON, IDVERSE

### Integrate today, revenue tomorrow

The ability to swiftly integrate new technology solutions is a key differentiator. Platforms that embrace automation demonstrate their commitment to innovation and agility, positioning themselves as leaders in the industry. They can quickly adapt to

#### \ Partner Spotlight \ New Partner Launch

Key Timeline Overview:



evolving market trends and customer demands, gaining a competitive edge and driving sustainable growth.

The integration of new technology solutions into partner platforms can be a complex and resource-intensive process. It involves thorough testing, validation, and often customization to ensure compatibility with existing infrastructure and regulatory requirements.

Fully automated identity verification systems leverage APIs to integrate and perform automatic updates in the future, compared to the need to replace SDKs over time.

### **Fewer vendors, more efficiency**

As businesses expand globally, they encounter a myriad of challenges in ensuring compliance, thwarting fraud, and delivering consistent user experiences. The traditional approach of relying on multiple identity verification suppliers complicates operations and increases the risk of human error and non-compliance. This is where the concept of consolidating IDV suppliers into a single, global solution emerges as a game-changer.

IDVerse's technology has been a game-changer for GeoComply in scaling our user onboarding process while significantly reducing the risk of onboarding fraudulent players. Its advanced solution allowed for instant verification of new players across any location and device, streamlining the onboarding process without needing manual intervention.

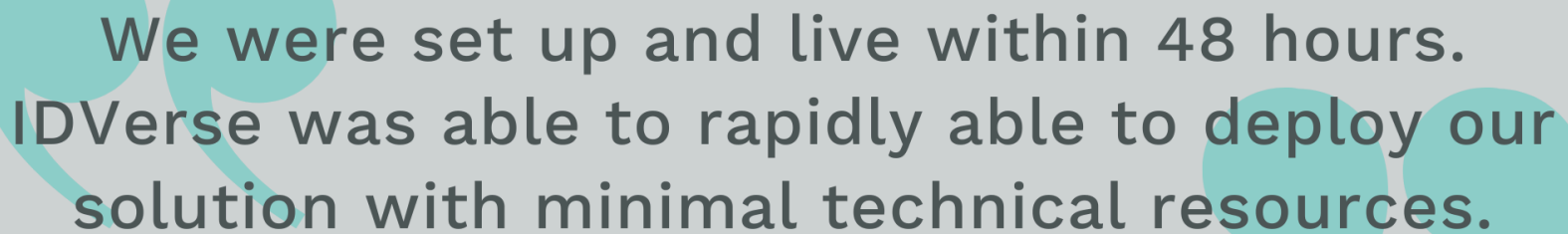
**AARON GOULD, VP OF IDENTITY, GEOCOMPLY**

Much like a universal translator breaking down language barriers, a global identity verification provider offers the versatility to verify documents issued by various jurisdictions in multiple languages,

accommodating the needs of customers worldwide. This consolidation streamlines operations and ensures consistency and compliance across various markets.

Think of an automated, AI-powered solution as an army combating fraudsters in real-time, analyzing documents with lightning speed and applying hundreds of checks instantaneously. Through the use of neural networks, these solutions continuously learn and adapt, ensuring that each verification process benefits from collective intelligence and experience.

With a single, global provider, businesses can consolidate their resources, reduce costs, and allocate resources more strategically. This consolidation also simplifies integration and maintenance, allowing for easy scalability as businesses grow and evolve.



We were set up and live within 48 hours. IDVerse was able to rapidly able to deploy our solution with minimal technical resources.

**TAAVI RIHVK & YORGEN MENESES, COINMETRO**

In the realm of identity verification, the future belongs to those who embrace innovation and collaboration. It's not just about adopting AI as a buzzword; it's about harnessing its transformative power to build a safer, more connected world.

## Scaling beyond bottlenecks

Platforms serve as crucial intermediaries in facilitating secure transactions and ensuring trust between businesses and consumers. However, as transaction volumes continue to rise globally, the scalability of identity verification processes emerges as a critical concern.

Manual or partially automated identity verification solutions rely heavily on human operators to review and authenticate identity documents and then compare them to selfies provided by users. These solutions inherently possess limitations in scalability, since human operators can only handle a finite number of verifications within a given timeframe. This leads to bottlenecks, delays, and a subpar user experience during peak periods of activity.

The fact that your DFA (Document Fraud Analysis) allows you to detect and distinguish each one of those specimens is really useful for us because we have customers from all around the world. The DFA works no matter what variation of ID is presented, if it is forged it will be correctly flagged, whereas a verification specialist may miss it.

**TAAVI RIHVK, COMPLIANCE LEAD, COINMETRO**

Consider the scenario of a major sporting event, such as the FIFA World Cup or the Olympics, where millions of fans from around the world engage in online transactions for ticket purchases, merchandise, and other related services. During such events, the demand for identity verification spikes significantly, overwhelming manual verification systems.

Similarly, retail events like Black Friday or new product launches witness a surge in online activity, driving up the need for swift and



intuitive IDV processes. Manual or partially automated solutions fall short in accommodating these sudden spikes in transaction volumes, leading to potential revenue loss, compliance risks, and reputational damage for platforms.

With the ability to dynamically allocate resources based on workload requirements, automated solutions ensure uninterrupted user experiences, minimize processing times, and mitigate the risk of transactional fraud.

### **Easing the technical lift**

An important consideration for platforms is the need for simple integration with their existing systems and workflows. Businesses rely on platforms to provide accurate and reliable identity verification services, and any disruptions or delays in the integration process can impact their operations.

A fully automated identity solution with API integration capabilities lets partner platforms ensure a smooth integration process for their clients, eliminating the need for additional headcount and technical resources.

### **Integrating brand continuity**

Consistency in branding ensures that users feel a sense of familiarity and reliability when interacting with identity verification services embedded within these platforms. This continuity in branding reinforces the legitimacy of the verification process and enhances the overall user experience by providing a seamless transition between different stages of the user journey.

Consistent branding also plays a pivotal role in reducing user journey drop-off rates and increasing conversion likelihood. When users encounter a disjointed or unfamiliar interface during the verification process, they may become hesitant or skeptical, leading to abandonment of the process altogether.

## Several ways to be a partner

At IDVerse we offer 3 partnership types:

1. **Introducer:** An Introducer Partner is an individual who makes introductions between IDVerse and people or businesses who potentially may require the IDVerse solution.
2. **Referrer:** A Referral Partner is an organization that refers IDVerse to its clients and is active in the sales cycle. IDVerse contracts directly with the client and pays the Referral Partner a referral fee.
3. **Reseller:** Incorporate IDVerse's core technologies into your own solution and provide this as a bundled service to end customers to service adjacent markets. A Platform Partner may also choose to engage as a Referrer or Reseller on a wholesale basis.

Which fits your business?

## 5. Growing Together



As partners, your collaboration with IDVerse isn't just about static benefits—it's about fostering mutual growth and innovation, ensuring that together we can reach new heights.

In this chapter, we'll look at how partnering with IDVerse facilitates this shared growth through various avenues.

### Complementary addition to your product suite

IDVerse understands the importance of synergy rather than competition. Partnering with us means adding a valuable component to your existing product suite without fear of overlap or redundancy.

Our solutions complement and enhance what you already offer, providing your customers with a more comprehensive and versatile set of tools.

### Fast time to revenue

Time is money, and with IDVerse, partners and their customers can accelerate their time to revenue significantly. Our enterprise IDV solutions are designed for swift integration, taking weeks, not months.

Furthermore, our API-driven approach ensures a hassle-free integration process, allowing partners to start seeing returns on investment in months, not years.

### Flexible solution models

One size does not fit all in today's diverse market landscape. IDVerse empowers partners to cater to the varied needs and sizes of their customer base.

Whether it's serving small and medium enterprises (SMEs), mid-market businesses, large enterprises, or government entities,

our solutions offer the flexibility to adapt and scale according to specific requirements. This flexibility enables partners to capture opportunities across multiple market segments effectively.

## Enable globalization

In an interconnected world, globalization is not just an option but often a strategic imperative for businesses. Partnering with IDVerse facilitates this process by offering solutions that align with your company's expansion goals.

Whether it's entering new markets or expanding operations in existing ones, our tools and expertise support partners in navigating the complexities of global business landscapes, helping them achieve their strategic objectives efficiently.

## Access to subject matter experts

Partnership with IDVerse grants access to a wealth of subject matter experts in various domains relevant to identity verification and related fields. Whether it's technical queries, regulatory compliance, or industry-specific nuances, partners can tap into our pool of experts for insights and guidance through various means:

- **Roundtables:** Partnership with IDVerse opens doors to exclusive roundtable discussions, offering a platform for invitation-only gatherings with industry peers. These sessions provide invaluable opportunities for partners to engage in strategic discussions, share best practices, and collaborate on addressing common challenges in the realm of identity verification.
- **Lunch & Learns:** We host educational sessions through Lunch & Learns, featuring subject matter experts in diverse fields. Partners have the opportunity to participate in sessions led by experts such as generative AI specialists or regulatory/compliance experts. These sessions serve to deepen partners' understanding of relevant topics, keeping



them abreast of the latest developments and regulatory requirements in the industry.

- **Webinars:** IDVerse organizes regular webinars featuring subject matter experts on various topics related to identity verification and cybersecurity. These webinars offer partners the chance to attend interactive sessions where they can learn about emerging trends, best practices, and innovative solutions from industry leaders. Partners gain valuable insights that can inform their strategies and enhance their offerings, ultimately driving mutual success.
- **Joint marketing campaigns:** We collaborate with partners on joint marketing campaigns to promote mutual offerings, generate leads, and increase brand awareness. These campaigns leverage the strengths and resources of both parties to reach target audiences more effectively and drive demand for IDVerse solutions. Partners have the opportunity to co-create marketing materials, participate in co-branded events, and leverage IDVerse's marketing channels and resources to amplify their message and reach new customers. By aligning their marketing efforts and messaging, IDVerse and its partners can maximize their impact and achieve greater success in the market.

In partnership with IDVerse, organizations can unlock new opportunities, reach wider audiences, and drive mutual success. Leveraging IDVerse's expertise and collaborative ecosystem, partners accelerate innovation, expand market reach, and deliver greater value to customers. This symbiotic relationship fosters dynamic growth and success in identity verification and cybersecurity.

## 6. Our Belief in Partnerships



At this point, we've discussed the new era of technology and fraud trends and why IDVerse stands as the pinnacle solution to combat these challenges.

As we wrap up this guide, let's reflect on the meaning of true partnership and how IDVerse is committed to building relationships that drive mutual success.

### True partnership is a two-way street

At IDVerse, we understand that partnerships are about more than transactions—they're about building lasting relationships. We seek partners who share our vision and values, and who are committed to delivering exceptional value to their clients. We can amplify our impact and create collective growth by aligning our goals and resources.

A true partnership is built on trust, transparency, and collaboration. We believe in open communication and mutual support, working together to overcome challenges and seize opportunities.

We view our partners as an extension of the IDVerse family, and we are dedicated to their success as much as we are to our own.

### Alignment of strategic goals

We work closely with our partners to understand their objectives and tailor our solutions to meet their specific needs. By aligning our strategies, we can create immense value for both parties.

With technology and customer needs evolving at a breakneck pace, future-proofing is crucial. IDVerse is committed to continuous innovation and improvement, investing in cutting-edge technologies and staying ahead of emerging fraud trends.

Our roadmap is designed to anticipate future challenges and opportunities, ensuring that our partners remain ahead of the curve.

## **Success through purposefulness**

We measure our success by the success of our partners. We are committed to providing the support, resources, and expertise needed to help our partners thrive. Whether it's through training programs, marketing support, or technical assistance, we are here to empower our partners at every turn.

Using technology for good is our core ethos, and we are committed to making the world a better place through our work. When you partner with IDVerse, you're gaining more than just access to a cutting-edge IDV solution; you are joining a movement to create a more inclusive and equitable future for all.

IDVerse is a versatile solution that can adapt to a wide range of use cases and industries. Whether you're in financial services, gaming telecommunications, or the public sector, our technology is designed to meet your unique needs and deliver exceptional results for your customers.

## **Unite against bias and fraud**

Fraud and risk management present enduring challenges that significantly affect businesses and individuals globally. This reality is particularly pronounced in an increasingly digital society, where customer interactions are predominantly remote and online.

Our commitment lies in addressing these challenges equitably, impartially, and inclusively. Leveraging the capabilities of AI and biometrics, we are forging a path towards a digital future that is both safer and more secure.

Partnering with IDVerse isn't just about accessing cutting-edge technology; it's about aligning with a collective committed to

driving positive change, where inclusion, fairness, and the mitigation of algorithmic bias are central pillars of our mission.

Get in touch with us today at **[partners@idverse.com](mailto:partners@idverse.com)** and let's build something meaningful together.

# Appendix

## 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    | <ul style="list-style-type: none"><li>NIST SP 800-171: Cybersecurity standards for protecting controlled unclassified information</li></ul>   |
| Advanced certification | <ul style="list-style-type: none"><li>NIST SP 800-53: Cybersecurity framework that provides guidelines for federal information systems</li><li>NIST SP-800 63 IAL 2: Cybersecurity standard that provides identity assurance in digital and online transactions</li></ul> |

#### iBeta/BixeLab against ISO 30107-3 (Biometric testing lab)

|                        |  |
|------------------------|--|
| Basic certification    | <ul style="list-style-type: none"><li>Liveness PAD Level 1: Basic presentation attack detection for biometrics</li></ul>   |
| Advanced certification | <ul style="list-style-type: none"><li>Liveness PAD Level 2: Enhanced presentation attack detection for biometrics</li><li>Liveness (bias testing): Testing for bias in biometric systems</li></ul> |

#### Government entities

|                     |  |
|---------------------|--|
| Basic certification | <ul style="list-style-type: none"><li>CPRA: California Privacy Rights Act for data privacy rights</li><li>GDPR: EU's General Data Protection Regulation for data privacy rights</li><li></li></ul> |
|---------------------|--|



|                               |  |
|-------------------------------|--|
| <b>Advanced certification</b> | <ul style="list-style-type: none"> <li>• TDIF L3: The Australian Government's Trusted Digital Identity Framework</li> <li>• DIATF: The UK Government's Digital Identity Authentication Trust Framework</li> <li>•</li> </ul> |
|-------------------------------|--|

## ISO (International Organization for Standardization)

|                               |  |
|-------------------------------|--|
| <b>Basic certification</b>    | <ul style="list-style-type: none"> <li>• ISO 9001: Quality management systems</li> <li>• ISO 22301: Business continuity management</li> <li>• ISO 29100: Privacy framework</li> </ul>  |
| <b>Advanced certification</b> | <ul style="list-style-type: none"> <li>• ISO 27001: Information security management</li> <li>• ISO 27017: Cloud security</li> <li>• ISO 27018: Cloud privacy</li> <li>• ISO 27701: Privacy information management</li> <li>• ISO 19795: Biometric performance testing</li> <li>• ISO 30107-3: Biometric presentation attack detection</li> </ul> |

## AICPA SOC (System and Organization Controls)

|                               |   |
|-------------------------------|---|
| <b>Basic certification</b>    | <ul style="list-style-type: none"> <li>• SOC 1: Financial controls audit</li> </ul>   |
| <b>Advanced certification</b> | <ul style="list-style-type: none"> <li>• SOC 2: Security, availability, processing integrity, confidentiality and privacy controls audit</li> </ul> |

## AICPA SOC (System and Organization Controls)

| Certifications                | Scope   |
|-------------------------------|---|
| <b>Basic certification</b>    | <ul style="list-style-type: none"> <li>• SOC 1: Financial controls audit</li> </ul>   |
| <b>Advanced certification</b> | <ul style="list-style-type: none"> <li>• SOC 2: Security, availability, processing integrity, confidentiality and privacy controls audit</li> </ul> |

## About the authors



**Libby Robinson** is Head of Partnerships for IDVerse. With over 12 years of experience in the identity and fraud space, Libby excels at developing partner ecosystems and helping companies understand the capabilities of IDV and fraud solutions. She has been with IDVerse since 2022 and is based in the London office.



**Matt Ingman** is VP, Partner Marketing for IDVerse. He has served in this marketing function since 2021 and has spent the last 7 years in the fraud and identity space. Matt brings a non-traditional way of thinking to deliver innovative and practical solutions for IDVerse's accelerated growth.



**Shane Tepper** writes about emerging trends in the world of technology with particular focus on generative AI and bias mitigation. With nearly 15 years of experience across media production, advertising, and the tech industry, he leads content marketing for IDVerse. Tepper is currently based in Atlanta.

## About the imagery

In our pursuit of innovation at IDVerse, we constantly push the boundaries of generative AI, seeking to unveil its potential across diverse applications. This ethos has guided our engineering, product, and marketing teams. It shapes our decision to integrate artificially generated visuals. Here, we embrace both the evident and concealed imperfections inherent in these creations, perceptible and imperceptible to the unaided eye. While human perception can discern the overt irregularities, the subtle anomalies existing at the nano-pixel level elude conventional observation, requiring the lens of computer vision for detection.

The inclusion of these images, with their conspicuous and covert flaws, serves as a metaphor for our world. It prompts contemplation on the constructs of normalcy and deviation, compelling viewers to adopt a new perspective. Through this, we endeavor to facilitate a deeper understanding, inviting audiences to transcend the surface and perceive the intricacies that lie beneath. Our aim is to encourage a paradigm shift, encouraging individuals to perceive beyond the superficial, fostering a richer engagement with the visual narrative presented.



In selecting rowing imagery for this guide, we aimed to represent the essence of collaboration and partnership. Rowing epitomizes the synchronized effort of individuals working together towards a common goal, mirroring the value of teamwork. Through these visuals, we illustrate our belief in the power of collective action and the strength that emerges when individuals work in concert towards shared objectives.

## About IDVerse

IDVerse, an OCR Labs company, 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 [partners@idverse.com](mailto:partners@idverse.com).



