IDVerse™

An OCR Labs Company

A WHITEPAPER FOR REMOTE IDENTITY VERIFICATION TECHNOLOGY

How to evaluate IDV technology and grow your customer base

2023

INTRODUCTION

Identity verification is the critical connective tissue between businesses and consumers everywhere. It's becoming table stakes in almost every industry, from financial services to employment to gaming.

Enabling as many consumers to access their goods and services as possible is how businesses grow. But in an online world, it's hard to do that safely while growing the customer base. When businesses aren't interacting with consumers face-to-face, they're exposed to greater risk of identity fraud. With businesses reporting the highest fraud rates in over 20 years,[1] they need to protect themselves and their customers by answering one simple question: are you who you say you are?

Businesses need to be cautious – but they also need to continue to onboard new customers. Finding the right balance between the two is an ongoing challenge. Done well, identity verification helps businesses onboard customers quickly, accurately and efficiently, and removes barriers to transactions further down the line. But done badly, identity verification can introduce friction, discourage sign ups, or even exclude certain user groups.

Remote Identity Verification (IDV) technology can help businesses onboard customers safely and seamlessly. In the last few years, a new wave of AI-powered software has come to the market to help businesses verify consumers' identities remotely and at scale. It's helped millions of people apply for online services, open bank accounts, send payments, share cars and homes, and verify social media accounts.

It's a rapidly-developing space. Adoption has grown thanks to the convenience IDV technology offers consumers, and the cost savings it delivers for businesses, which would otherwise need large teams of trained staff and physical facilities to verify identities. It

[1] https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

accelerated again during the COVID pandemic, as in-person identity verification became more difficult, and more businesses moved online. Post-COVID, underpinned by long standing secular shifts towards the digital economy, the need for remote identity verification continues.

But not all IDV technology is created equal. Different risk levels, business contexts and regulatory requirements need different solutions. To adequately protect themselves while servicing the widest possible audience, businesses need to understand how IDV technology works, whether it will meet the real needs of clients and legitimate consumers, and how well it will manage risk in their system. Evaluating IDV solutions should therefore be seen not just as a tick-the-box exercise, but a raise-the bar-initiative.

In this whitepaper, we will explore the key components of IDV technology, and how businesses should evaluate solutions to find best-fit.

KEY TAKEAWAYS

1. **Synthetic fraud and deepfakes are getting harder to catch:** Identity fraud is not only becoming more common, but more sophisticated. Professional criminals are developing ever-more complex ways to get around businesses' defenses, including synthetic fraud and generative AI (deepfakes). Faced with this mounting threat, robust IDV is not only nice to have, but essential. Manual techniques are no longer fit for purpose: businesses need to invest in AI-driven IDV software to keep up with fraudsters, and keep themselves and their users safe.
2. **Bias in identity systems is being scrutinized:** Several countries and governments have begun to develop regulations for algorithmic bias, recognizing the potential harms and negative impact of biased decision-making systems. These regulations may vary in scope and approach, but generally aim to promote fairness, accountability, and transparency in the design and use of AI-based

identity decision-making systems.

3. **IDV solutions aren't 'one size fits all':** Different classes of IDV solutions offer different functionalities and levels of protection. Businesses need to create their own evaluation framework, and select the solutions that are most appropriate to their own risk appetite.
4. **Bias is a major blocker to IDV performance:** Bias can creep into IDV systems in a number of ways. The most significant is algorithmic bias, which is a key concern for solutions that leverage AI. Businesses should look for Zero Bias solutions in order to ensure inclusivity and accessibility across global user bases.
5. **IDV solutions need ongoing operational support:** IDV solutions require ongoing, expert management to protect against evolving fraud techniques, while keeping systems fair and equitable. Building a robust approach to Identity Operations (IDOps) is the best way to future-proof businesses.

UNDERSTANDING IDV TECHNOLOGY

Various IDV technologies exist. Typically, digital camera systems, computational imaging, and 3D sensing technologies are coupled with advanced software algorithms to capture and analyze images or videos. These tools allow for more sophisticated and accurate identity verification, as well as improved performance in low-light or challenging environmental conditions.

The steps in remote IDV

There are four steps in the IDV workflow:

1. **Optical Character Recognition (OCR)**: OCR software uses advanced optical character recognition algorithms to analyze the features of an identity document, including human-readable and machine-language symbols, and determine its authenticity.
2. **Document Fraud Analysis (DFA)**: The DFA process involves the use of advanced algorithms to perform comprehensive analysis of the physical and security features of the document (including the printing quality, color accuracy, security features, and layout) in order to determine the authenticity of the document. It also checks for watermarks, holograms, and other security features that are difficult to replicate.
3. **3D Liveness Detection (3DLD)**: The user is asked to perform a specific action, such as blinking or smiling, during the selfie video capture process. This verifies that the user is physically present, and not just submitting a pre-recorded photo or video.
4. **Face Matching (FM)**: The user is asked to take a selfie photo or video, which is then compared to the photo on their identity document. This verifies that the person in the photo is the same as the person who provided the identity document.

Table 1: Steps in Remote IDV

Step 1	Step 2	Step 3	Step 4
Convert an image containing text into a machine-readable text format	Distinguish between genuine and fraudulent identity documents	Determine “liveness” or genuine presence of an individual in a selfie photo	Match the individual in a selfie photo to a photo ID or other authoritative image

How IDV technology works

But how do these processes actually work? At the front end, users submit one or more identity documents (such as a passport, driver's license, national ID card, or other government-issued identification), and a selfie photo or video. At the backend, IDV systems utilize three types of data processing to determine their validity.

Table 2: Backend IDV Document Processing

I. DOCUMENT PROCESSING	
Calculative sub-processing types:	
Alignment check	Verifies that the text and images on the document are properly aligned to that document's standard.
Comparison to text on	Verifies that the information on the document matches the text on

the front/back	the front/back of the document.
Typography check	Verifies the consistency of the typography used on the document.
MRZ/PDF 417 check	Verifies the validity of the Machine-Readable Zone (MRZ) or PDF 417 barcode on the document against OCR information.
Graphical sub-processing types:	
Color management check	Verifies that the colors used on the document meet the specifications.
Font color check	Verifies that the font color used on the document meets the specifications.
Hologram check	Verifies the presence and validity of any holograms that are required on the document.
Symbol check	Verifies the presence and validity of any symbols or logos that are required on the document.
Forensic sub-process types:	
Deepfake image check	Verifies if the image has been manipulated using deepfake technology.

Digital aspects check	Verifies the digital aspects of the image, including its origin and traces of image manipulation or reconstruction.
Synthetic ID check	Verifies if the ID is synthetically generated.
Tampering check	Verifies if the document has been tampered with at the file or physical level.

Table 3: Backend IDV Liveness Processing

II. LIVENESS PROCESSING	
Biometric liveness sub-processing types:[2]	
Deepfake video check	Verifies if the video has been manipulated using deepfake technology.
Environmental lighting	Verifies whether lighting in background matches light refraction on face presented.
Skin textural check	Verifies the presence of a person by looking for live skin properties.
Spoof check	Verifies if there are deception attempts in the video using physical elements such as masks, screens, printed materials etc.

[2] Evaluating if one or more distinguishing biological traits is from a live person present at the point of capture.

Table 4: Backend IDV Face Match Processing

III. FACE MATCH PROCESSING	
Face matching sub-processing types:[3]	
Bias removal	The application of mathematical models to ensure inclusion and fairness (zero bias), and protect against algorithmic bias or systemic discrimination.
Measure facial features	Verifies that the measurements of the face in the document and face in the selfie/video have the same measurements.
Multiple frame check	Verifying that a number of frames match the document face image from the video.

The role of AI in IDV

Underpinning all of these processes is Artificial Intelligence (AI). AI is now ubiquitous in IDV technology, and with good reason. AI can help IDV systems to detect fraud, and improve the user experience by making the verification process faster and more accurate. It's particularly valuable for businesses verifying high volumes of identities, where human intervention is less practical or effective.

AI-based identity verification systems use machine learning algorithms and deep neural networks to analyze and learn from vast amounts of data and detect patterns that could

[3] The ability to scan, recognize and compare human faces to images presented in identity documents.

indicate fraudulent behavior. This can include identifying fake identities, detecting manipulated or stolen documents, and analyzing behavioral biometrics to ensure that the user is who they claim to be.

AI systems are also faster than humans. By automating document and facial checks, they enable businesses to process a large volume of verifications, and onboard or re-authenticate consumers quickly and seamlessly.

But AI is a broad term. It can mean many different things, and be deployed in different ways to drive different outcomes. And it's constantly evolving. Below are some of the latest AI techniques being leveraged in the IDV process, and the potential value they add for businesses:

- **Zero Bias AI**: This technology ensures that face matching and liveness validation are independently evaluated. A key concern with AI-based IDV systems is that they may not perform well for everyone. Communities who have difficulty obtaining certain ID documents, or whose facial features do not match the algorithmic models used by the software, may be incorrectly flagged or rejected by the system. Zero Bias AI makes IDV more **inclusive** and **accessible.**
- **Full Image Context Processing**: This technology uses the full document image, surrounding background context, and metadata to verify the identity of an individual. Full Image Context Processing makes IDV more **comprehensive**.
- **Federated Intelligence**: This technology uses networked data to allow multiple parties to collaboratively train a machine learning model, without sharing their private data with each other. Federated Intelligence makes IDV more **accurate**.
- **Collaborative Machine Learning**: This technology uses multiple decentralized devices or servers holding local ID data to perform liveness validation, without the need to move or copy data. Collaborative Machine Learning makes IDV more **secure** and **private**.
- **Contextual Machine Learning**: This technology allows for the adaptation and application of models to different scenarios and situations. Contextual Machine

Learning makes IDV more **adaptable**.

EVALUATING IDV TECHNOLOGY

In order to effectively evaluate IDV solutions and make sound investments, businesses need to understand not only *how* IDV systems work, but *how well* they work.

Accuracy and effectiveness in reducing identity fraud at scale is impacted by a number of variables, both inside and outside the business. Failure to implement the right IDV solution can have serious repercussions. Technology that is too light-touch can put businesses at increased risk of identity fraud and non-compliance. Technology that is too heavyweight may result in consumers being incorrectly identified as fraudsters, and left unable to access services.

Businesses considering IDV technology should create their own testing and evaluation framework to ensure the accuracy, fairness and effectiveness of solutions. This framework should extend past the point of purchase. Ongoing monitoring and dedicated resources will be required to identify and correct any biases or inaccuracies, and comply with evolving regulations.

In order to effectively evaluate solutions, it is critical to clearly establish business context, goals and priorities. IDV technology is not-one-size fits all, and not a silver bullet. Businesses should think carefully about whether they have the maturity, financial and human resources to manage and optimize solutions. Investment in the widest feature set and latest technology is wasted if it doesn't clearly answer business needs, or is too complex to integrate and maintain.

There are several things to consider in determining which solutions are most appropriate. Below are some helpful questions to ask

- What is your risk appetite?
    - This may be dependent on your industry, the type of goods and services you sell, and business priorities around speed, scale and security.

- What are your compliance requirements?
    - IDV regulation differs across industry and geography.
- Who are your users?
    - Users in marginalized or underprivileged communities may require different IDV systems and workflows.
- What is your user journey?
    - Are you using IDV to onboard new users, re-authenticate users, or both? Different workflows may be required at different trigger points.
- How mature is your organization?
    - The more sophisticated the IDV solution, the more technical resource and cross-functional collaboration will be required to keep it functioning optimally.

Having established their own goals, businesses should look to the following criterias to assess best-fit.

Certifications

IDV solutions can be certified by a range of independent and governmental bodies, each of which test to their own standards. Some certifications are basic, while others are more rigorous and harder to obtain.

Checking certification can be a good place for businesses to start. In some instances, businesses will be obliged by clients or local regulators to use an IDV system with particular certification or capabilities. For instance, to be a US Federal Governments Instant Payments provider, businesses would need to have data protections in place "consistent with industry benchmarks set by organizations such as the National Institute of Standards and Technology (NIST).[4]" Likewise, landlords, letting agents, and employers

[4]https://www.frbservices.org/binaries/content/assets/crsocms/financial-services/fednow/prepare-fo

in the UK are now encouraged to use IDV providers that can prove they align with the UK Digital Identity and Attributes Trust Framework (DTIAF).[5] To provide IDV services to the Australian Government, solutions must be Trusted Digital Identity Framework (TDIF)[6] accredited.

Table 5: Checklist of Certifications for IDV Technology Providers

Certification Body	Basic-Level Certifications	Advanced-Level Certifications
NIST	NIST SP 800-171	NIST SP 800-53
iBeta/BixeLab against ISO 30107-3	Liveness PAD Level 1	Liveness PAD Level 2 Liveness (bias testing)
Government Entities	CCPA, GDPR	TDIF L3, DIATF, 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 System and Organization Controls (SOC)	SOC 1	SOC 2
Web Content Accessibility	Level A	Level AA / AAA

r-fednow/fednow-service-readiness-guide.pdf
[5]https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/outcome/government-response-to-the-digital-identity-and-attributes-consultation
[6] https://www.digitalidentity.gov.au/tdif

Guidelines (WCAG)		

NOTE: *Within certification levels, there can be variances in performance. For example, IDV solutions can be certified for Liveness PAD Level 2 if they achieve error rates within a range of 0 - 20%. Advanced-Level IDV providers can attain closer to a 0% error rate for their FNMR (Face Non Match Rate) or BPNR (Bona fide presentation non-response rate).*

Maturity

After certification, there are some simple indicators businesses can use to assess an IDV solution's level of maturity and complexity. Among other things, these can help determine whether it is capable of handling a wide range of identification documents from different regions and languages – which is important to ensure consistency of experience in scaling, global businesses.

Below are some of the key indicators to check, and why they matter:

- **Years in Operation**: indicates whether the system has time to mature and develop its capabilities.
- **Number of Customers**: indicates whether it is trusted by a large number of organizations and individuals.
- **Yearly Transaction Volume**: indicates whether the system can accommodate a large amount of data.
- **Requires Human/Manual Screening**: Indicates how highly automated and efficient the system is, especially at processing large volumes of transactions.
- **Countries/Territories Supported**: indicates whether the system has a broad international reach, and is capable of handling a wide range of identification documents from different regions.
- **Languages/Type Fonts Supported**: indicates whether the system is capable of

handling a wide range of identification documents from different cultures and languages, eg. non-Latin scripts (Greek, Chinese, Japanese, Hebrew).

- **Document Type Library Size**: indicates whether the system has a comprehensive database of identification documents, and is capable of handling a wide range of identification document types, eg. passports, drivers licenses, national identity cards.
- **Technology Ownership**: indicates whether the system roadmap, functionality and issue resolution is fully controlled by the business themselves, or they are reliant on 3rd parties to provide their service.

Classification

The above two steps should help businesses create a long list of potential solutions. But certification and maturity metrics alone are not enough to assess best-fit. Businesses also need to determine the type and level of functionality they need from their IDV solutions. There are three classes of IDV solutions. It's important to carefully consider the capabilities of each, to ensure that it is appropriate for business-specific application, and that it meets with security and privacy requirements.

Class 1: Static Identity Verification

Class 1 IDV solutions are typically used for low-risk transactions, where the consequences of a false match are minimal. An example might be accessing public transportation.

Typically, Class 1 solutions rely on 1-to-1 matching of a consumer's face to their photo. They use biometric authentication to compare a selfie photo to a government-issued ID photo.

Class 1 Capabilities:

- **Document Detection and OCR:**
    - Image of a document is analyzed
    - Country/province and document type is automatically identified
    - Printed data is extracted, contextualized, and made available for auto-filling forms and input screens
    - Barcodes or machine-readable zone (MRZ) properties are extracted and compared with the printed data.
- **Face Matching (1:1)**:
    - Image of face from selfie is compared with image of face from ID document
    - NFC enabled documents i.e. passports are matched against NFC stored image
    - Low quality face images and age variation can be matched effectively.
- **Static Liveness / Presentation Attack Detection**:
    - Static image of face is analyzed using textural analysis to identify printouts, masks and screen captures.

Class 2: Dynamic Identity Verification

Class 2 IDV capabilities are typically used for higher-risk transactions, where the consequences of a false match are more significant. An example might be unlocking a phone or computer.

Class 2 IDV solutions include automated, dynamic, and adaptive techniques, and use real-time videos and motion. They use liveness detection to verify that the user is physically present, and not using a static image or video to bypass the system.

Class 2 Capabilities:

- **Document Fraud Analysis**
    - Document is checked for authenticity, tampering and security features, including:

        - Barcode analysis, alignments of card elements, typography type, spacing and consistency, symbols, colors, holograms, font color
        - Textural analysis, ensuring document image isn't from a screen, photocopy or reprint
        - Tamper checks for specific damage, wear and other known attack vectors such as lifted film, text scratching, artificial or chemical wear.
    - Image of face from document is checked against specifications for size, boundary, background and graphical elements or overlays
    - Document is checked to ensure it is not a synthetically generated ID, deepfake manipulated image or “photoshopped” image.
- **Face Recognition Velocity (1:N / One to Many)**:
    - Image of face from selfie or video is matched to faces within a very large dataset, enabling one to many face matching or face recognition
    - Various factors are examined which might not be suspicious in isolation, but become suspicious when taking place within a certain timeframe (velocity checks).
- **Dynamic Liveness / Presentation Attack Detection**:
    - Captures real time video
    - Supports multi-language localization
    - Provides accessibility features for written and voice prompts.

Class 3: Outcomes-Focused Identity Verification

Class 3 IDV capabilities are typically used for transactions wherein it is important to maintain consumer trust, and ensure technology is used in a responsible and ethical manner. Examples might include country border crossing, employment screening, providing financial services, college admissions, and home rentals.

Class 3 IDV solutions consider the system's outcomes or impact on each user's rights, opportunities, or access to critical services. They include features that ensure zero bias

fairness, transparency, and accountability, such as bias testing, audit trails, and data privacy protections.

Class 3 Capabilities:

- **Global Coverage**:
    - Supports wide range of countries/territories, languages/typefaces, and document types
        - **Countries/Territories**: The number of geographic regions where IDV systems are available. This reflects the reach of the technology, operations, and ability to serve customers in different parts of the world.
        - **Languages/Typefaces**: The different languages and character sets the IDV system supports. This is particularly important in regions where multiple languages are spoken. It reflects a company's commitment to serving diverse populations, and making its products accessible to as many people as possible.
        - **Document Types**: The different types of documents (identification cards, billing invoices, legal contracts, medical records, financial statements, etc) the IDV system supports. This reflects a technology's ability to serve a wide range of industries and business types, and can be important for companies that operate in highly regulated or specialized industries.
- **Algorithmic Discrimination Protections**:
    - Protects against algorithmic discrimination when developing AI systems (refer to "Bias" section below for more information).
- **Automated**:
    - Does not require manual or human screening. To achieve automation, IDV systems need the following attributes:
        - **End-to-end Capabilities Integration**: Combines document

validation, biometric recognition, and liveness detection in one user session.

- **Scalability**: Automatically scales up or down to handle changes in usage and traffic.
- **Usage-based pricing**: Is cost-effective, and only charges for the actual usage of the system, not idle resources.
- **Secure Architecture**: Provides a secure and reliable environment for running code. The system is designed to only expose the necessary endpoints, and implements security measures to ensure that sensitive data is protected.

Table 6: Classification of IDV Capabilities

<table>
<tr><th rowspan="2">IDV
CLASS</th><th colspan="3">IDV Capabilities</th></tr>
<tr><th>Document Validation
(OCR & DFA)</th><th>Match to ID
(FM)</th><th>Liveness
(3DLD)</th></tr>
<tr><td>CLASS 1</td><td>Document Detection and OCR (Autofill)</td><td>Face Matching (1:1)</td><td>Static Liveness (Selfie Photo)</td></tr>
<tr><td>↓
Enablers (AI)
↓</td><td>↓
Full Image Context Processing
↓</td><td>↓
Federated Intelligence
↓</td><td>↓
Collaborative Machine Learning
↓</td></tr>
<tr><td>CLASS 2</td><td>Document Fraud Analysis (DFA)</td><td>Face Recognition Velocity (1:N)</td><td>Dynamic Liveness (Selfie Video)</td></tr>
<tr><td>↓
Enablers (AI)
↓</td><td>↓
Contextual Machine Learning
↓</td><td colspan="2">↓
Zero Bias AI
↓</td></tr>
<tr><td rowspan="2">CLASS 3</td><td>Global Coverage
(Countries/Territories
x Languages
x Document Types)</td><td colspan="2">Algorithmic Discrimination Protections*</td></tr>
<tr><td colspan="3">Automated</td></tr>
</table>

*Regulatory guidance from the White House Office of Science and Technology Policy's Blueprint for an AI Bill of Rights

Bias

AI is a critical enabler for every class of IDV technology. But as the table above shows, it becomes more complex and more important as solutions become more sophisticated. Businesses need to approach AI with sensitivity, and ensure they and the systems they use have good data hygiene. Otherwise, they won't perform optimally, and could create more problems than they solve.

Inclusive IDV technology has the power to support underserved groups in society. By removing barriers that lead to exclusion, digital ID systems can ensure that as many people as possible have access to life-enhancing products and services. But if poorly designed, not every consumer will have a fair and equitable experience. Ensuring that IDV technologies work effectively regardless of race, ethnicity, sex, gender identity, age, national origin or disability, is essential.

Bias can creep into IDV in a number of ways. **Language bias** can occur if IDV solutions only support Latin scripts, for instance. The Latin Script is used to write English and at least 150 other languages, spoken by 70% of the world's population. But more than 2 billion people use another writing system, and are at risk of exclusion if front-end instructions and back-end document processing don't recognise them.

Likewise, **system bias** can negatively impact marginalized communities, such as those without access to the latest technology, or those with disabilities. If systems only work on the latest smartphone model, with a superior camera spec, or with a high speed internet connection, billions may be excluded. If IDV solutions rely on voice recognition, this can be challenging for those with speech impediments.

But the most significant risk comes from **algorithmic bias**. Algorithmic bias usually arises from data bias. AI models are only as good as the data used to build them. Put simply, poor inputs will yield poor outputs. If the data used to train AI models is not diverse and representative of the population, it can result in errors in the model's predictions and decisions. Women and ethnic minorities are most at risk from this type of bias. In 2018, a study from MIT[7] revealed that facial recognition error rates for white men were less than 1 in 100. For dark-skinned women, the error rates were 1 in 3. The solutions surveyed were found to have been developed using data sets containing 77% male images and 83% white images. However, algorithmic bias can still occur even when the data itself is unbiased. If algorithms aren't designed to account for factors that may disproportionately affect certain groups or populations, they risk being excluded.

Best Practices to Reduce Bias

Accessibility and inclusivity should be a priority (and is a legal imperative) for all businesses. Assessing for bias is therefore an important step in the evaluation process. Even if a vendor has excellent technology, its value will be limited if any group of people is systematically excluded from using it. There are a number of principles businesses should look for in order to determine how well IDV technology providers manage and mitigate bias:

1. **Obtaining Independent Lab Evaluation**: Having independent labs evaluate the AI system can help to identify and address any biases or discriminatory patterns that may be present. This can include evaluating the system's performance across different demographic groups, and identifying any disparities in outcomes.
2. **Using Representative Data**: To avoid bias and discrimination against age, gender or race, it is important to use data that is representative of the user communities the system will serve. This includes using diverse training datasets, and ensuring

[7] https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

that the data includes a broad range of experiences and perspectives. Data should also be reviewed for bias based on the historical and societal context of the data.

3. **Making a Commitment to Zero Bias:** Establish a code of ethics for systems development that includes a commitment to zero bias. This should be followed by all members of the development team, including data scientists, programmers, and other stakeholders.
4. **Providing Transparency and Accountability:** Make the decision-making process transparent and provide explanations for the system's predictions. This can help build trust with users and stakeholders.
5. **Regularly Testing and Auditing:** Regularly test and audit systems to ensure that they are free from biases and assumptions. The testing should be performed on diverse and representative data.
6. **Continuously Improving:** Continuously improve based on feedback from users and stakeholders. The system should be updated with new data and new techniques to ensure that it remains unbiased and accurate.

Outputs

IDV system outputs are equally important as functionality and inputs. Managing identities and access across IT resources is becoming very challenging for many businesses, especially as the volume of users and devices grows. Ensuring that outputs are appropriate and actionable within specific business contexts is integral to their success.

Risk assessment engines look different inside every business, and that means the information they need to make decisions is different, too. The system outputs for IDV solutions can vary, and need to be carefully matched to use cases.

There are three typical outputs from IDV solutions:

1. **Validity Outcome***: boolean (true, false)*

Validity outcomes are simple yes/no answers. Outputs are expressed as a boolean value, indicating whether the identity verification was successful or not.

Validity outcomes are best suited to relatively low-risk transactions, where the consequences of a false match are minimal.

2. **Validity Score**: *numeric value (0.0 - 1.0)*

Validity scores add more context to validity outcomes, by indicating the level of confidence in the decision, e.g. yes with 95% confidence. Outputs are expressed as a floating-point number between 0.0 and 1.0, indicating the confidence level of the verification result.

Validity scores enable businesses to exercise more control by setting a cutoff point based on their own risk appetite. They may choose to reject verifications with <90% confidence, for instance.

3. **Validity Properties**: *key-value pairs (InformationFormatCorrect, InformationCorrect, InformationComplete, CheckSumsCorrect, MRZCorrect, PhotoTampered, LivenessCheck, InformationCompleteness, SecurityFeaturesTampered, DataFieldsTampered, etc.)*

Validity Properties offer the most detailed response, and can be helpful in high-risk scenarios, where businesses need a robust audit trail. They are used to explain the ‘why’ behind validity outcomes and validity scores, eg. no with 95% confidence because liveness check failed due to deepfake detection.

Validity properties can include information about the correctness, completeness, and integrity of the information provided, as well as any tampering or security issues detected during the verification process.

Performance and Metrics

Naturally, performance metrics play an important role in understanding the quality of IDV solutions. But they should not be considered in isolation, because they can be impacted by a number of variables. IDV solutions, especially those powered by AI, will perform optimally if they are strategically managed throughout their lifecycle. Businesses need to ensure they have the expertise and operational capacity to monitor, improve, and test solutions on an ongoing basis. Otherwise, performance will be impacted.

It's also important to understand which metrics to track. Below are the key metrics to measure, and industry benchmarks which can be useful to inform evaluation. Performance measurements should be tested in accordance with biometric industry standards, and verified by recognized, independent labs:

Table 7: Document Accuracy Metrics

Metric	Meaning
Document False Accept Rate (DFAR)	Measures the percentage of fraudulent or invalid documents that are incorrectly accepted by the system. A low number indicates that the system is less likely to accept fraudulent or invalid documents.
Document False Reject Rate (DFRR)	Measures the percentage of valid documents that are incorrectly rejected by the system. A low number indicates that the system has a high level of

	accuracy in recognizing valid documents.
Document Processing Time (DPT)	Measures the time it takes for the system to process a document and provide a verification result. A low number indicates that the system is fast and efficient.
System Error Rate (SEC)	Measures the overall error rate of the system, including errors in document validation, identity verification, and other system processes. A low number indicates that the system has a high level of accuracy and reliability.

Table 8: Liveness Accuracy Metrics

Metric	Meaning
Bona Fide Presentation Non-Response (BNPR)	Measures the proportion of bona fide presentations that cause no response at the presentation attack detection (PAD) subsystem or data capture subsystem.
Failure To Acquire (FTA)	Measures how often the system fails to capture a sample from the subject.

Failure To Enrol (FTE)	Measures how often the system fails to enroll the subject.
False Non-Match Rate (FNMR)	Measures the Proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample.
Impostor Attack Presentation Match Rate (IAPMR)	Measures the proportion of impostor attack presentations using the same presentation attack instrument (PAI) species in which the target reference is matched.

Table 9: Biometric Face Matching Accuracy Metrics

Metric	Meaning
Failure To Acquire (FTA)	Measures the proportion of verification or identification attempts that fail because the system fails to capture a sample.
False Acceptance Rate (FAR)	Measures the proportion of impostor transactions that are accepted by the system.
False Match Rate (FMR)	Measures the proportion of impostor matches that are falsely matched.
False Non-Match Rate (FNMR)	Measures the proportion of genuine matches that are falsely non-matched.

False Rejection Rate (FRR)	Measures the proportion of genuine transactions that are rejected by the system.
System Stability to Race and Gender (Bias)	Measures the system's ability to perform equally well for users of different races and genders. A low number indicates that the system is unbiased, and does not discriminate based on race or gender.

CONCLUSION

Quality IDV solutions can add enormous value to businesses, and add firepower to their efforts to fight identity fraud as they scale. That's why it's so important to implement a rigorous evaluation and testing framework before committing to investments.

To make it easier and ensure all the important factors have been taken into consideration, businesses can use the checklist below:

- ☐ **Certifications:** Are you obliged by clients or regulators to implement IDV solutions with specific certifications, eg. NIST, SOC?
- ☐ **Maturity:** Are you satisfied that solutions are established and mature enough to meet and grow with your business needs?
- ☐ **Classification:** Are you clear on the risk appetite of your business, and do solutions offer the appropriate level of protection?
- ☐ **Bias:** Are solutions adequately mitigating bias, and do you have the internal resources to monitor and manage bias into the future?

- ☐ **Outputs:** Are you aware of the system outputs that the different teams across your business require in order to manage risk effectively?
- ☐ **Performance:** Are you monitoring the most important metrics, and do you have the internal capability to optimize them?

The final point is essential. Thinking beyond the point of purchase to ensure there is cross-functional communication, buy-in and operational support for IDV systems will give businesses the best chance of success.

Identity Operations (IDOps)

Identity Operations (IDOps) is an emerging approach that combines the domains of identity verification, operations, and machine learning to improve the lifecycle of identity-related processes. It foregrounds collaboration, continuous improvement, and adaptation to improve performance and create efficiencies.

By leveraging advanced machine learning techniques, IDOps can learn from user interactions, identify patterns and anomalies, and adapt to changing requirements and environments. This helps improve the quality and accuracy of identity-related processes. With IDOps, organizations can reduce errors, improve security, and enhance the user experience.

With identity fraud on the rise, businesses that can integrate thoroughly-evaluated IDV solutions into strategic IDOps frameworks are best-placed to not only survive, but scale. Businesses need a strong understanding of the ever-evolving identity fraud landscape, and to know that their IDV solution is designed to tackle risk and optimize outcomes.

About IDVerse

IDVerse lets you scale your business to the world. Our identity verification products automatically verify new users in seconds with just their face and smartphone - in over 220 countries and territories.

Through our quest for Zero Bias AI™ 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.

To find out more about how we help customers grow their businesses, read our report on *The Truths About Identity And Inclusion.*

Visit: www.idverse.com
Email: hello@idverse.com