Your Face is Data — and Scammers Are Using it for Fraud. Here are 5 Tips When Using Identity Verification

Opinions expressed by Entrepreneur contributors are their own.

Historically, many organizations deployed identity verification (IDV) procedures to meet regulatory requirements in their particular niche. However, its applications are now more varied, including processes that have already become routine for many of us: secure customer onboarding, remote hiring facilitation, online transaction safety on marketplaces and gig economy platforms and fraud detection.

This diversity of tasks complicates choosing IDV solutions, challenging the one-size-fits-all approach across different industries. Despite this, certain key considerations can guide the evaluation process beyond the usual factors like industry and company size.

What to look at first?

1. Does the solution cover all of the essential steps of the IDV procedure?

Most of the IDV solutions on the market include document and biometric verification steps, which represent the core of identity verification. The document verification step includes document capture, document assessment and data extraction for

further verification. The biometric part typically includes selfie capture and face matching.

Can you measure the effectiveness of document and biometric checks? Absolutely! For instance, you can use the retake score – the need to redo the verification process, which arises when the initial attempt falls short of clarity or fails to satisfy established criteria – to evaluate the document and/or selfie capture modules.

However, there is a catch. Despite many vendors making similar claims, it's critical to consider the sampling used to measure these scores as they relate to software performance. For example, a developer may claim they have a 100% OCR accuracy – perfect effectiveness of Optical Character Recognition technology to accurately read and convert text from identification documents into digital form. High accuracy is crucial for capturing data correctly and minimizing errors throughout the verification process. But how do you know if this figure is not based solely on cases involving a specific single document type, such as German passports or Louisiana driver's licenses? If you work only with documents issued in those geographies, you will be fine. But will the same accuracy apply to documents from the United Arab Emirates, for instance?

Qualitative indicators also need to be taken into account. Advanced IDV software must properly validate all security features. In practice, it should handle all types of Machine Readable Zone (MRZ) codes (lines of encoded data typically found at the bottom of passports and identity documents, designed for easy scanning and processing by machines), recognize and extract data (including photos) from different barcodes and other parts of the document. Additionally, it should be able to scan the NFC chip containing the user's identity details and send the information to a secure server managed by the entity conducting the identity verification, ensuring the identity is valid and secure. This two-step

process helps prevent fraud.

The comprehensiveness and accuracy of the document template database are also super important, as it is used for identifying the large variety of existing identity documents, including passports, driver's licenses and residence permits.

Related: The 'Mother of All Breaches' Just Happened – Here's the Security Implications for Businesses

2. Does the solution recognize modern types of fraud?

AI-enabled attacks like deepfakes are a growing threat that organizations can no longer ignore. Regula's global survey shows that approximately 80% of companies worldwide think that various types of deepfake fraud are a real threat. These are artificially generated images, videos or audio that highly realistically mimic real people.

A recent instance involved the Hong Kong branch of a multinational company, which lost $25 million after a scammer used deepfake technology to impersonate the firm's chief financial officer (CFO) during a group video conference call, instructed staff to transfer funds.

Not surprisingly, businesses and governments perceive the identity fraud detection capabilities of an IDV solution to be one of the most crucial selection criteria.

It is imperative to understand how the vendor confronts the deepfake threat by asking precise questions about the relevant features. For instance, inquire about the software's capability to detect various types of presentation attacks – when a fraudster presents fake, altered or otherwise manipulated biometric samples (like facial images, video or voice recordings) to deceive and gain access through a biometric security system – and the mechanisms it employs to

unveil them.

You may also want to assess how the solution tackles the particular types of identity fraud employing deepfakes. Fraudsters may display a fake photo or video of a “live” person on a secondary device at the selfie stage. For proper identification, the software should be able to detect static face images, electronic devices, video replays and video injections.

Related: Facial Recognition Technology Is Streamlining Check-in Processes – and Raising Privacy Concerns

3. Does the vendor’s development strategy reflect current changes in the market?

Businesses’ demands, end users’ expectations and industry standards are changing. With the emergence of new ID formats like digital identities and mobile driver’s licenses, vendors have to consider these verification scenarios when bringing their solutions to the market.

For this reason, flexibility and technological competence have become crucial criteria when assessing IDV developers. For instance, mono solutions that only verify domestic documents seem out-of-date in the era of global migration, digital nomadism, remote customer onboarding and online transactions. With physical document fraud still prevalent, robust IDV systems must include a complete set of authenticity checks, like document liveness – a verification method used to ensure a document is original and not forged or altered, typically checked through real-time presentation or authenticity features.

The vendor’s product development roadmap is the right starting point to gain the required insight. The roadmap visualizes the

vendor’s strategic plan, showing the details of upcoming improvements and features that will roll out soon.

Related: Deepfakes Are on the Rise – Will They Change How Businesses Verify Their Users?

4. Are your customers fully satisfied with the IDV flow?

A customer-centric approach is now at the core of many business processes, including identity verification. A better customer experience (CX) is both a driver and success determiner for many organizations implementing IDV solutions. Regula’s survey finds that customer satisfaction improvements were the main reason for 29% of companies deploying such solutions. Additionally, 55% of business representatives named improved CX as the top success indicator for IDV.

Usually, it’s up to you to decide how to smoothly embed the IDV solution into your current processes. However, interoperability, cross-platforming and customization features are the sole responsibility of the developer. As a quick rule of thumb, cross-platform solutions that perform well on websites and in mobile apps enable you to set up a seamless IDV flow that enhances customer satisfaction.

Automation is also a cornerstone of a customer-centric approach. Both clients and employees will appreciate it if they can skip routine parts of the IDV process like data entry or document type detection.

For instance, Skylegs, an aviation management platform, reports positive client feedback after it implemented IDV software for aircraft operators. With data entry automation, the operators can now process passports and ID cards more easily, faster and more accurately.

5. Does the solution enhance ROI for your IDV investment?

Evaluate an IDV solution as a strategic investment that impacts numerous outcomes. As an example, the Canadian travel solution Sherpa cut annual operational costs by 15% after IDV automation.

Identity verification is more than simply authenticating documents and individuals; in most instances, multiple adjacent use cases exist in any given company. A solid all-in-one IDV solution can help businesses reduce security risks, comply with KYC requirements and increase customer satisfaction.

The completeness of a given solution often implies broad coverage of diverse IDV use cases. The solution must be versatile enough to cover many industries, from regulated ones like Aviation, Gambling and Banking, to more unconstrained businesses like eLearning or eCommerce.

By favoring single-vendor solutions, covering all aspects of IDV from biometrics to document verification, you get comprehensive and easy-to-maintain software as a bonus. First, all the updates will be applied universally, instead of piecemeal. Second, you will be protected against asynchronous updating, in which one of the modules loses interoperability with all the other systems because of mistiming by one of the developers.

A bonus piece of advice: The dataset matters

IDV vendors usually offer a demo or trial period to test the waters. You can try out various solutions and assess how their products accomplish your tasks. Some businesses test out

solutions using the vendor’s datasets. This approach may seem a bit biased, which is why the number and variety of specimens available for testing, as well as the level of detail in the verification results, are also important criteria to consider.

However, many organizations prefer “real data” involving physical IDs volunteered by employees from a focus group. To make the most out of this experience, you need to prepare your dataset properly.

First, it should match your company’s demands. If you deal with identity documents issued in the UK only, you can simply scan and verify the passports of your British volunteers during the test. But the results will be inadequate if identity documents from other countries like Germany, UAE and Italy also flow into your systems.

Second, your dataset should be complete to provide statistically valid metrics. As mentioned above, to obtain accurate measurements for all four scenarios, you would need an equal number of passports from British, German, UAE and Italian individuals.

In conclusion

Measuring the success of an IDV solution helps businesses ensure they are achieving their desired outcomes. By considering indicators such as customer feedback and ROI, companies can gain valuable insights into the effectiveness of their IDV solution. It’s also important to regularly monitor these indicators and make adjustments as needed to optimize the solution’s performance.

https://www.entrepreneur.com/science-technology/5-things-to-consider-when-evaluating-id-verification/472715