A Buyer’s Guide to Online Identity Verification

How to Evaluate Vendors in the Emerging Trusted Identity as a Service Space

FINANCIAL SERVICES EDITION
Identity verification is the process of verifying that a person is who they claim to be. Identity verification is a common practice for the financial services industry for remote bank account opening and AML/KYC/BSA compliance.

Unfortunately, on the Internet, it’s hard to know if someone’s digital identity matches their real-world identity. Your customer could be a dog, a money launderer, a fraudster, or a legitimate customer just trying to transact or open an account.

Because of cybercriminals and routine data breaches, trust is in increasingly short supply. In response, online companies are often forced to add steps (translation: added friction) into the sign-up process.

As trust evaporates, the market for identity proofing has exploded and new solution providers have rushed in to help fill the void. In this increasingly cluttered marketplace, it’s difficult to separate the pretenders from the contenders.

While no one solution can meet every bank’s needs, this guide will help you:

- Uncover important information about the identity verification market
- Learn how to compare solutions
- Identify essential functional requirements based on your unique needs
- Understand key considerations for your purchase decision
- Learn how to perform a competitive bake-off

We will walk through the trade-offs companies often have to make between deterring fraud and increasing conversion rates. We will explore the steps businesses can take to mitigate risks and the identity proofing technologies that can be brought to bear to establish trust, detect fraud, and increase assurance that someone is who they say they are.
The Fraud Detection User Conversion Matrix

Historically, organizations have been forced to make tough trade-offs when addressing identity verification. They could either have higher levels of fraud detection which necessarily adds incremental friction to attain higher levels of identity assurance. Conversely, they could opt for higher levels of conversion rates which often meant reducing the friction during the account setup process (which, in turn, translated to lower levels of assurance). So, pick your poison—higher levels of fraud detection with lower conversion rates or opt for higher conversion rates with lower levels of fraud detection/assurance.

This matrix below illustrates this once difficult tradeoff.

The vertical access measures the level of fraud detection required to lower an organization’s risk exposure. Note: This goes beyond just fraud detection and includes a variety of risks such as economic (how much money was stolen), compliance (fines imposed for compliance lapses) and/or reputational (impact on brand and consumer trust).

For some financial services organizations, it may be more important to onboard as many new customers as possible with as little friction as possible. If you’re a retail, brick and mortar bank, for example, you can expand your digital footprint with a secure, remote identity verification. While no organization is comfortable with fraud, some financial service companies may prioritize user conversions over fraud detection and may be willing to write off some level of fraud in the pursuit of more customers.
In Search of Identity Verification Nirvana

Ideally, a solution could offer both high levels of fraud detection with high conversion rates. But, this requires incremental functionality. In the chart above, adding identity and document verification to core ID verification solutions can enable more companies to add layers of identity assurance and fraud detection with minimal friction.

For many financial institutions today, the only way to ensure high levels of fraud detection is to require a customer to physically visit a branch office. But modern smartphone-enabled technologies are enabling more organizations to achieve identity verification nirvana—high levels of fraud detection coupled with high user conversion rates. But, in order to do this, identity verification solutions must have the right combination of features, technologies, and processes.

Two Types of Verification Accuracy

The fraud detection-user conversion matrix underscores that there are two types of verification accuracy that organizations care about.

- How well can the solution catch fraud (catch fake or doctored IDs, pictures used instead of an actual selfie, etc.)?
- How well does the solution convert users (i.e., verify your good users)?

Depending on whether you’re looking to detect as much fraud as possible or convert as many users as possible, you need to inspect to see if your identity vendor has the right set of features and functionality to support your unique needs.
Your Verification Options

Once upon a time, the Internet was a more anonymous space. People hid their real identities, coming up with unique and sometimes bizarre pseudonyms to represent themselves on specific websites. But as consumer services and socializing shifted online, establishing a person’s real-life identity digitally became increasingly important.

The desire for anonymity hasn’t completely disappeared. But, as the social web has grown, people have become more accepting of using their ‘real’ identities online. At the same time, large scale data breaches from Verizon to Forever 21 to Equifax, have compromised customers’ PII (personally identifiable information) data.

So, how can you verify someone’s real world identity online, without impacting users’ experience? The table below provides a summary of the more popular online verification methods, each with their associated pros and cons.

<table>
<thead>
<tr>
<th>Verification Method</th>
<th>Defined</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge-Based Authentication (KBA)</td>
<td>KBA verifies customers by asking them to answer specific security questions in order to provide accurate authorization for online or digital activities.</td>
<td>• Well understood by users</td>
<td>• Easy to discover answers via social networking sites and social engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Questions gathered over the course of 30 years</td>
<td>• Fraudsters can buy KBA answers on the black market</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Questions must be answered within defined time limit</td>
<td>• Generated questions often based on credit bureau info</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Recent data breaches exposing PII</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Limited to certain countries</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Often delivers a poor user experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Does not rely on government-issued IDs, it lacks a certain degree of authority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Some customers find this line of questioning intrusive</td>
</tr>
<tr>
<td>Two Factor Authentication (2FA)</td>
<td>Two factor authentication is an extra layer of security that requires not only a password and username, but also something that the user has on them (i.e. a piece of information only they should know or have immediately on hand, such as a physical token or a numeric code delivered via text message).</td>
<td>• Out-of-band (independent channel) authentication</td>
<td>• Vulnerable to key logging, SMS-spoofing, man-in-the-middle and man-in-the-browser attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Strong deterrent (fraudster must possess secondary token)</td>
<td>• NIST declared SMS-based 2FA insecure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Near ubiquitous penetration of smartphones</td>
<td>• Bad customer experience if you lose one of your authentication factors (smartphone, key fob)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Regulations such as PSD2 driving wider adoption</td>
<td>• Can be slow and cumbersome</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Effective verification for account opening and password resets</td>
<td>• Users must have their second factor (smartphone, key fob) with them at all times</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Requires extra typing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Too easy for an inattentive user to approve an attacker’s transaction without knowing it</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reliance on third-party services (either authentication service providers or telecom companies) is also a factor to consider, since breaches in these services have in the past resulted in authentication failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Additional points of failure</td>
</tr>
<tr>
<td>Verification Method</td>
<td>Defined</td>
<td>Pros</td>
<td>Cons</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Credit Bureau-Based Solutions            | Many online identity verification systems call out to one of the big three credit bureaus, Experian, Equifax, and TransUnion, who then search for an identity match within their vast repositories of consumer credit data. | • Authoritative databases provide a wealth of information based on first and last name, address, and social security number  
• Easy API implementation  
• Definitive match provided (vs. a score)  
• Unintrusive customer experience  
• Fast results | • People with thin credit files, usually young people, recent immigrants, or people who for some reason have very rarely used mainstream financial services, often cannot be matched  
• Does not verify that the person providing the information is the actual person behind the transaction  
• Less reliable with false positives when common names are used  
• Fraudsters increasingly have access to credit bureau data thanks to several recent breaches  
• Does not rely on government-issued IDs, it lacks a certain degree of authority  
• Implementing companies often have to state that a credit bureau check is performed in the Ts and Cs which can creates headaches  
• Some customers do not like having the credit bureaus pinged because of the footprint it has on their credit file  
• Limited geographic coverage |
| Database Solutions                        | These solutions leverage online, social media, and offline data (and sometimes behavioral patterns) to detect if an online ID is authentic, a fraudster or a bot. | • API-based  
• Analyzes a variety of data from different sources to verify identity  
• Significantly reduce the number of manual reviews  
• Often used for risk monitoring | • Can be spoofed because of the ease of creating fake online identities (e.g., synthetic identity fraud) and bogus social profiles  
• Does not verify that the person providing the information is the actual person behind the transaction  
• Does not rely on government-issued IDs, it lacks a certain degree of authority  
• Often confidence score provided; not a definitive yes or no  
• Often does not meet compliance/regulatory requirements |
| Online Identity Verification              | Often leverage a mix of artificial intelligence, computer vision, and verification experts to determine if a government-issued ID is authentic and belongs to the user. These solutions often perform validity checks via a selfie to ensure that the person holding the ID the same person shown in the ID photo. | • Variety of AI, biometrics, machine learning, and human review used to assess legitimacy of ID and identity  
• High verification assurance  
• Relies on valid government-issued ID and selfie to verify identity  
• KYC, AML and BSA compliance  
• API, SDK and Webcam implementations  
• Definitive yes/no result provided  
• Verification results usually provided within a few minutes | • Requires user to capture a photo of their ID and take a selfie (introduces some friction)  
• Speed of verification, especially for manual reviews  
• Geographic coverage and ID support (for some vendors)  
• Limited geographic coverage and ID support  
• Additional verification information is typically not provided |
Because of the recent well-publicized data breaches, there is a growing chorus that knowledge-based authentication has become wholly inadequate as a verification method. More and more companies are exploring how can they evolve past KBA to alternative verification methods to reliably and accurately establish someone’s online identity with higher levels of assurance and confidence.

ID verification with biometric facial recognition is showing considerable promise to be the logical successor to KBA. By combining ID verification with a complete identity (biometric-based) verification, emerging online identity verification solutions can ensure the person is physically who they say they are and have possession of the documentation to prove it.

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include eyeball tracking, fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. These methods become important because they help ensure that the person behind an online transaction is live (not a picture) and that the person behind the biometric matches the one identified in the government-issued ID.

The remainder of this Buyer’s Guide will focus on how to select the best online identity verification solution and how to better grade the solution providers in this space.
Key Verification Features, Technologies & Processes

To help you better assess where a verification vendor sits on the fraud detection-conversion rate matrix, it’s helpful to understand the underlying key features, functionalities and processes that can help improve fraud detection and user conversions.

All too often, organizations evaluate vendors on a limited set of purchase criteria (e.g., price per verification, geographic scope). But, there’s a fair amount of nuance in what different solution providers bring to the table that asking a vendor to explain their machine learning processes or whether they support older versions of state-issued driver’s licenses or ID cards in specific countries, will make you a smarter, savvier buyer.

The table of key features below can be an instructive guide to finding the right verification solution. Each of the features and functionalities is described in detail on the following pages.

<table>
<thead>
<tr>
<th>Feature/Functionality</th>
<th>Fraud Detection</th>
<th>User Conversion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Learning</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Data Tagging</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Auditing Verifications</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Liveness Detection</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Geographic Coverage</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>ID Version Support</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Expired IDs</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>KYC, AML &amp; BSA Compliance</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Fraud Database</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Database of Valid Users</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Human Review</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Trend Spotting</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Barcode &amp; MRZ Scanning</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Omnichannel Support</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Blur &amp; Glare Detection</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>PCI Compliance</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Black &amp; White ID Detection</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Document Verification</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Getting a Definitive Answer</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
1. Machine Learning @ Scale

Machine learning (ML) is used by many ID verification solutions, so you often have to dig into their process for training the algorithms. It starts with the size of their database of good and bad (i.e. fraudulent) transactions. The larger the dataset, the smarter the algorithms. Machine learning models can be created for many different use cases, such as blur detection and bad image quality detection which requires a large volume of good transactions to better train the algorithms. Some solution providers literally fake the data and will use computer programs to take a single sample image and then make hundreds of variants of that ID (which, unfortunately, do not simulate the real world). Make sure you understand the volume and scope of an identity verification provider in terms of the number of global verifications they have performed.

2. Data Tagging

While big data is important, you also need to have the data intelligently tagged. Some vendors leverage verification experts to tag IDs—both good and rejected images—to help train ML algorithms, tagging the images based on:

- Was the image scuffed?
- Was the ID hole punched?
- Which country was the ID from?
- Was there glare?
- Was part of the picture obscured by a thumb?

By tagging tens of thousands of IDs in this manner, the algorithms that feed machine learning get smarter, faster and learn how to recognize these patterns automatically.

3. Audited Data

Without auditing the verification history, the only way to know if they’re getting it right is by having their customers catch and notify them of incorrect verifications. Look for solutions that audit 10-20% of transactions to ensure that their verification engine is correctly flagging fraudulent IDs and green-lighting your good customers in a timely manner. With machine learning becoming so integral to modern verification solutions, the audit serves as a powerful check to improve system accuracy and ML algorithms.
4. Liveness Detection

Increasingly biometric facial recognition is being used to combat fraudsters who attempt to use static images or a pre-recorded video to “fake” their identity. A common problem with smartphone-based solutions is fraudsters can simply take a picture of an ID and using that image as proof of their identity. With biometric facial recognition and liveness detection better identity solutions can combat fraudsters who attempt to use static images to “fake” their identity.

It’s important that these liveness checks don’t take too long or become too onerous for legitimate users.

By embedding liveness detection into the account setup process, financial services organizations can significantly impact fraud without impacting the customer experience. Just the requirement of taking a selfie will often have a chilling effect on would-be fraudsters who don’t want their actual likeness captured for posterity.

5. Geographic Coverage

Depending on the geographic diversity of your user base, this may or may not be an important consideration. What’s important is whether your provider can support the countries, languages, and ID types of your user community. It’s not just a matter of driver’s licenses and passports, you may also want to support ID cards as well. Most of the larger identity verification players can support multiple countries because they can read the MRZ on passports, but many of them cannot support other ID types (e.g. ID cards).

6. ID Version Support

Another important consideration is a solution provider’s ability to support all the possible versions and permutations of a particular state’s driver’s license. In some cases, there may be as many as 15 versions of a particular driver’s license—some issued 5 years ago, some issued 10 years ago, some printed in landscape, some in portrait, some for commercial drivers and some for driver’s permits—each with their own unique set of security features.
7. Expired IDs

Many DMVs and passport offices use a hole punch to mark a license or passport as invalid. The most common time this is done is when you renew your license/passport, and they punch the old one.

Since the one you’re looking at is not expired, it’s been invalidated for another reason. Most likely, the license was suspended and the individual was issued a non-driver ID or a restricted DL in its place. The department punches holes in your invalid passport before sending it back to the user, officially canceling it. A canceled and returned passport cannot be used for identification in any circumstance, including passport renewal. Unfortunately, many ID verification solutions cannot detect hole punches in drivers licenses and passport because of the limitations of their ML algorithms. The lesson is, make sure your identity verification solution can detect and invalidate IDs with hole punches.

8. KYC, AML and BSA Compliance

New regulations not only accept that electronic means of ID verification are as valid and trustworthy as in-person identity verification, but stresses the advantages of electronic ID and identity verification for account opening, record keeping, and high-value transactions monitoring.

When done via a smartphone or desktop webcam, identity verification based on ID document authentication presents an elegant solution for complying with Know Your Customer (KYC), Anti-Money Laundering (AML) and Bank Secrecy Act (BSA) regulations without inconveniencing customers. Modern online identity verification solutions go beyond verifying the authenticity of a government-issued ID. They confirm the presence of the account holder. When the customer takes a selfie with their smartphone, the selfie image is compared instantly to that of the ID document tying the ID to the owner in real time, at any time and from anywhere.

9. Fraud Database

If an ID has been flagged as fraudulent (e.g. it’s been doctored or digitally manipulated) and it is used again, modern solutions will capture this in their own databases. The more transactions, the more fraud captured, the larger the database, and the greater its potential impact. Much like machine learning, when it comes to fraud, sometimes it’s the company with the largest fraud database that wins the day. With some of the larger players in this space who manage global brands, they will see the same fake ID show up across different web properties. This scale enables them to quickly identify and reject repeat offenders on the fly.
10. Database of Valid IDs

Having a large database of known fraudsters is obviously helpful in terms of fraud detection and preventing those fraudsters from using the same bogus ID credentials across multiple online properties. But, the opposite is true too when it comes to capturing legitimate and genuine government-issued IDs. If a verification solution has a large database of known, legitimate users that can streamline the verification process, but only when paired with a battle-tested identity (face-matching) solution. If a valid ID is stolen, online companies need a way to verify that the person behind the ID matches the ID being put forth to establish identity. When only a government-issued ID is required, fraudsters can hide behind its anonymity. But, when a selfie or some type of biometric is required, most fraudsters will move on to other targets not willing to forsake that same anonymity.

11. Human Review

The fact is humans can often see patterns that automation and machine learning can’t. But, there’s a pretty steep learning curve when it comes to visually inspecting IDs from around the globe. Just consider the number of global IDs, each template embedded with a unique set of security features, data positions, font types (and font size), and other distinct characteristics. This expertise takes time to learn, so make sure to ask how large is the verification team, how experienced, how are they trained, and how long has the team been in place.

In addition to understanding the makeup of the manual verification team, you should also ask how long does it take, on average, to complete manual/human review. Unfortunately, for many solution providers new to human review, these teams can take hours—not seconds or minutes—to successfully complete a manual review. This is critical to onboarding new customers and new bank accounts with minimal abandonment during the signup process.

12. Trend Spotting

Let’s say a fraud ring figures out how to doctor Nepalese driver’s licenses. For most automated solutions, it would take some time to hard code the logic into its algorithms. The more transactions captured by a identity verification provider, the more business intelligence baked into their solutions, and the more nimble the solutions (in terms of processes to alert human reviewers), the faster these companies can identify and respond to fraud patterns. Global solution providers that verify millions of transactions each year are better positioned to identify these patterns in real-time and adapt quickly since the verification teams can be instantly alerted to pay special attention to Nepalese driver’s licenses.
13. Omnichannel Support

Many ID verification solutions only support smartphone image capture and exclude other channels such as desktop webcams. By excluding webcams, these vendors are excluding large market segments who are more comfortable on their desktop and laptop computers. A significant share of online verifications are based on images captured by webcams depending on the application and use case. Being omnichannel also means supporting API-based, mobile web and native mobile implementations. For companies looking to cast the widest possible net, including some older people who may not be comfortable with newer technology, it just makes sense to ensure that your identity verification solution offers the broadest number of channels to your users.

14. Blur & Glare Detection

While the cameras embedded within today’s smartphone provide crisp, high resolution pictures. Unfortunately, this is not true for older phones or for photos captured with many webcams. If you allow webcams for image capture, you need a way to alert your users/customers when the image is blurry, fuzzy, or just has too much glare so they can retake the picture and course correct. Blur detection provides that functionality and lets financial service organizations modify thresholds to meet their needs.

15. Barcode & MRZ Scanning

Most ID and Identity solution providers can read the barcode on the backside of driver’s licenses and the MRZ (machine readable zones) on passports. A user’s first and last name, date of birth, and contact details can quickly be extracted from the barcode/MRZ. But, how well does your identity provider read these areas if the barcode or MRZ is damaged or unreadable? Does the identity vendor check to make sure the data extracted from the barcode/MRZ matches the information on the front side of the ID and/or match the picture to the selfie taken?
16. PCI Compliance

The Payment Card Industry Data Security Standard (PCI DSS) requires companies that accept credit cards to host the data securely with a PCI-compliant hosting provider. Unfortunately, only a handful of verification solution providers are PCI compliant and have had their policies, processes, and controls independently tested to ensure that credit card or PII data is handled in a secure manner. This also means that the verification vendor extracts, redacts (masks), and stores merchant’s credit card information while adhering to PCI DSS, reducing customers’ internal processing and operational costs.

17. Black & White Detection

Over the years, the regulatory authorities have tried all manner of tactics to combat fake driver’s licenses and passports. Holograms. Water marks. Since all legitimate IDs are issued in color, it’s important to only accept colorized IDs and be able to detect which ones are, in fact, black and white. Black and white images are often copies of the original ID but can be doctored.

**NOTE:** Some government IDs may use sepia or black and white photos, but the IDs themselves are always in color.

While most of the leading identity solutions can distinguish black and white images from color images of government-issued IDs, it’s important to make sure this box gets checked too.
18. Document Verification

Online document verification allows businesses to quickly extract data from supporting documents such as utility bills and credit card and bank statements using their smartphones. This information can add an additional layer of identity proofing and ensures that a user is who they claim to be. Look for solutions that can extract data in less than ideal circumstances like scanning crumpled documents. Better solutions have the ability to extract Latin-based (including those written in English, French, Spanish and Italian) and Chinese characters to include broader document support.

19. Getting a Definitive Answer

Most organizations don’t have the personnel or requisite skillset to get a list of suspect transactions. What most companies want, and usually demand, is a definitive “yes” or “no” that tells whether they should accept or reject the user. More importantly, better verification solutions will return additional information about why an ID was rejected (e.g., because the photo taken was a photo of a computer screen) or why an selfie was not accepted (e.g., because the selfie is actually a photo cropped from the physical ID).

These extra details are exceedingly valuable for banks and financial service organizations to improve conversion rates and lessen the friction of its users. With a simple “yes” or “no” solution, these good users would be rejected out of hand without given the chance to course correct. Unfortunately, many online solutions return only a score. For many automated solutions, online verifications fall into three categories—clearly good, clearly bad, and a large middle-ground of gray (or “iffy”) transactions. Better hybrid solutions rely on human review to better verify the suspect transactions and improve overall verification accuracy.

While this list is by no means constitutes a complete list of questions that you will want to ask a would-be identity verification provider, it’s a good start and will help you assess the maturity and experience of the vendor. In addition to these questions, we encourage customers to road test a short list of vetted identity verification providers to see how accurate and how complete these solutions are.
The proof is in the pudding. Solutions that employing cutting edge technologies, machine learning, and biometrics, coupled with well-trained human review, should yield the highest verification accuracy—both in terms of fraud detection and user conversions. But, the only real way to test this is to perform a competitive bake-off (assuming you want to go beyond reference checks).

So, how do you conduct a fair bake-off?

Instead of providing a prescriptive plan for how to perform ID/identity verification testing, we will provide a handful of best practices to test, really test, an identity verification solution.

1. **Compare apples to apples.**

Make sure the vendors that you’re comparing offer similar types of identity verification solutions. It doesn’t make much sense to compare a database solution to an online identity verification solution unless the use cases and outcomes are comparable.

2. **Have a representative sample.**

The bake-off should take advantage of a large dataset, not just a few transactions, but ideally include thousands of transactions that will lead to comparatively better, more representative samples. In addition to a large percentage of legitimate IDs/identities, businesses may send the solution provider 10-20 fraudulent IDs, to simulate real world transaction volumes.

3. **Test legit IDs as well as fake ones.**

Because many financial services organizations care just as much about optimizing user conversions as they do about detecting fraud, it’s important to test a large sample of legitimate IDs to see how well each vendor correctly identifies them as good. Remember, fraudulent transactions typically make up less than 1% of total transactions. Having the right mix of legitimate and fraudulent transactions will help you gauge each vendor’s ability to correctly identify both good and fake IDs. Based on our own benchmark tests, many automated solutions are no better than a coin toss at correctly identifying legitimate IDs and this means they often deny legitimate IDs because they were taken with under less than optimal conditions.
4. Test under less-than-ideal circumstances.

When it comes to capturing IDs and identity selfies, make sure to include sample IDs that were taken with bad lighting, with blurred or glared images, and with folded or bent IDs. Again, the goal should be to simulate the real world as closely as you can and, the fact is, your users will take pictures of their IDs and of themselves under less than ideal circumstances.

5. Test for expired IDs.

When a passport or driver’s license is expired, the issuing agency will usually punch a hole through it. Many automated verification solutions won't actually capture these expired IDs which is a glaring loophole in any verification solution.

6. Test for older or different versions of an ID.

Don't just test with the current year’s model of a driver’s license. In many cases, users will have older IDs, commercial driver’s licenses, and even paper-based driver’s licenses (still used in some European countries) and the better identity verification solutions will be able to capture and verify all legitimate forms of ID -- not just a recently issued ID. You may even want to check to see how well the vendor does when the selfie includes two or more people or pictures with users and their pets. Believe it or not, these are the types of pictures that people include during the verification process so you should know how well your vendor can discern these nuances.

7. Check to see that a reason code is issued with denied verifications.

For many online identity verification providers, failed verifications are returned without including a reason code that explains why a verification was denied. This is not helpful. Better solutions return a reason code that allows the business and, more importantly, the user to course correct. For example, if the image of an ID was too blurry or there was too much glare, the business can ask the user to retake the picture so they can complete the verification process.

8. Test international IDs.

Naturally, if you’re a global bank or even a regional brand that has customers in a few countries, you should ensure that your test includes a variety of IDs from those countries. Because of barcodes (driver’s licenses) and machine readable zones (passports), many ID verification solutions can verify the most common ID types in the countries you operate, but in order to cast the widest possible net, it’s important to test ID cards, older versions of driver’s licenses, and IDs in different languages to ensure that your solution provider can capture and accurately extract and verify those IDs.
9. Test with a black & white IDs.

There are no legitimate ID types that are completely black and white. While some may feature a black and white photo, the driver’s license or ID card itself will be in color. Better online identity verification solutions will be able to detect and deny black and white IDs.

10. Test the time it takes to receive a verification result.

It’s not just about accuracy, you should also measure how long it takes to get a verification result. Many automated solutions will boast a verification SLA measured in seconds, but when put into production, the actual response times are much slower. The benefit of testing with production data is that you can see in real-time just how long it takes to get a response back from the vendor.

11. Test the speed of manual reviews.

Many solutions are adept at reading driver’s licenses and passports because they’re only reading and extracting information from the barcode and MRZ, respectively. But, as soon as the verification goes into the “gray zone” and they get reviewed by human verification experts, the response times go from seconds to hours to sometimes days.

12. Audit the results.

This probably goes without saying, but a big challenge with testing in the wild is knowing how well each vendor performed in flagging fraudulent IDs/identities and passing legitimate users. If you’re using production data, make sure to include some fake/bogus IDs to see how well each vendor caught those bogus IDs. Then, you should be able to review the reason code reports for each vendor to see how well they did at passing legitimate users.
In the emerging ecosystem of identity verification, it’s difficult to separate signal from noise. On the surface, many of the players in this space sound the same and boast many of the same capabilities. That’s why savvier banks and financial service organizations are starting to ask tough questions and dig into the genuine capabilities of a vendor.

While it’s probably a no-brainer that accuracy matters when it comes to online ID and identity verification, it’s difficult to know which vendors are more accurate—where do they excel and where do they fall short. At the end of the day, what matters most is how accurate can they spot fraudulent IDs and how fast can they greenlight the verification process for your good customers. Both measures of accuracy are important.

In this Buyer’s Guide, we outlined the fraud detection/user conversion matrix—a model that assumes there are tradeoffs between identifying fraud and optimizing user conversions. We outlined the key features, technologies and processes to determine which solutions will better detect fraud and which ones will convert more legitimate customers.

While understanding which vendors offer each of these technologies is helpful, the best way to test the claims of accuracy and speed of a given verification solution is to test it, but under real-life circumstances. To this end, we provided 12 best practices for performing a competitive bake-off and encourage you to develop a testing plan that leverages as many of these practices, so you can make a confident, data-based decision on the best online identity verification solution for your needs.
Thanks to data breaches, cybercriminals, and compliance mandates, it’s never been harder or more important to establish trust online.

As traditional methods of verification, including simple passwords, knowledge-based authentication, database solutions, and credit bureaus have proven vulnerable, governments, regulators, and enterprises are being forced to find more robust, secure, and reliable verification methods to definitively establish identity.

Connecting a person’s online and real-world identities is the sweet spot of Jumio.

Whether in front of a webcam or a smartphone, we can quickly verify the authenticity of an ID, a document, or your customer’s real-world identity in seconds—not hours or days—helping you optimize account openings, deter fraud, and meet AML, KYC, and BSA compliance mandates while providing a fast, seamless customer experience.

Jumio uses computer vision technology, machine learning and live verification experts to verify credentials (e.g., passports, driver’s licenses, etc.) issued by over 200 countries. Our technology powers businesses with scalable, secure and compliant identity verification, which enables them to build and sustain trust in an increasingly unsafe digital world.

Jumio is widely considered to be the largest and most accurate solution in the market and used by leading companies in the financial services, cryptocurrency, sharing economy, retail, travel, and online gaming sectors.

Based in Palo Alto, California, and funded by Centana Growth Partners and Millennium Technology Value Partners, Jumio operates globally, with offices in the US, Europe, and Asia Pacific and has been the recipient of numerous awards for innovation, including this year’s Frost & Sullivan’s North American Entrepreneurial Company of the Year for the Biometric Security Solutions Industry.

When identity matters, trust Jumio.