

A BUYER'S GUIDE to Online Identity Verification



How to Choose the
Right Solution and Features

jumio®

Do you (really) know your customer?

Identity verification is the process of verifying that a person is who they claim to be. Identity verification is a common practice used across industries for common tasks such as renewing a driver's license, securing new employment or opening a bank account.

Unfortunately, on the internet, it's hard to know if someone's digital identity matches their real-world identity. Your customer could be a fraudster, a money launderer, an underage minor – 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 identity proofing steps into the sign-up process, which can add unwanted friction and lead to higher drop-off rates.

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.



What's in this guide?

This guide will help you:

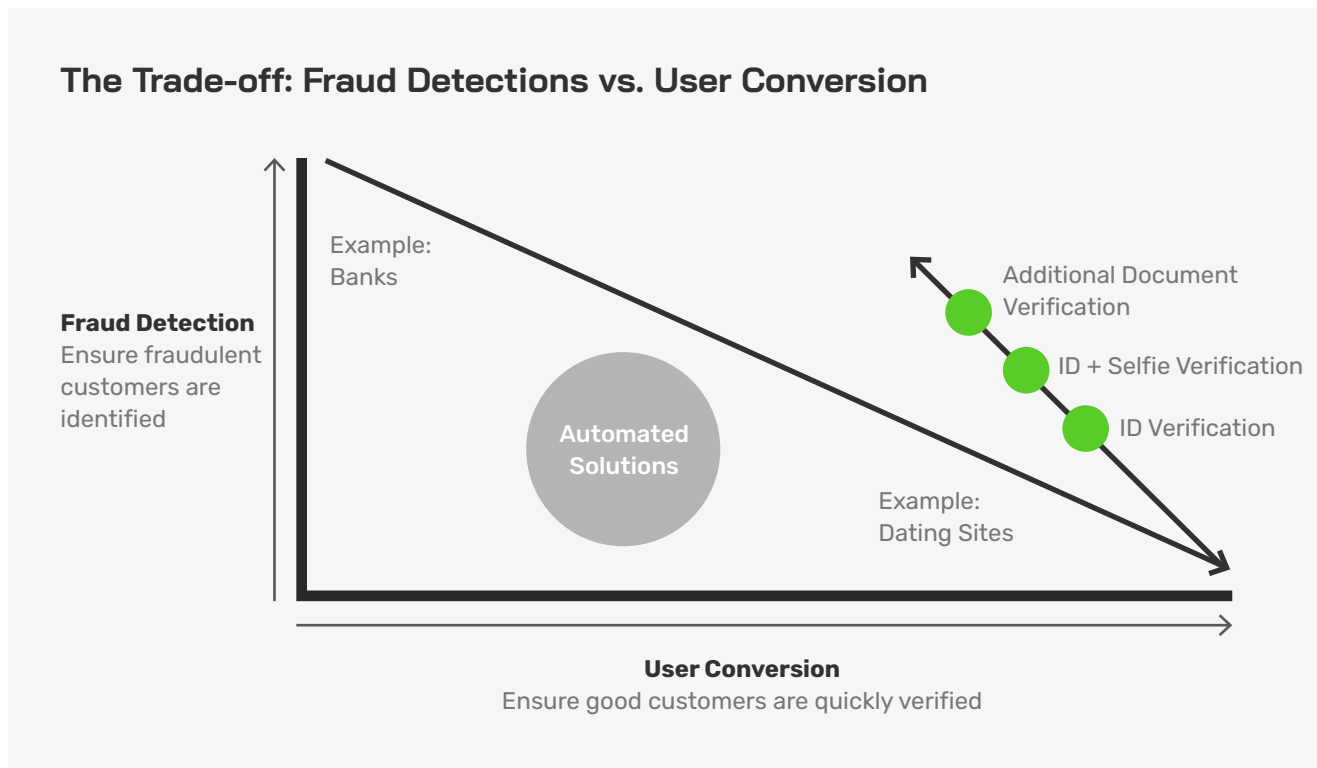
- ✓ **Uncover important information about the identity verification market**
- ✓ **Understand verification options**
- ✓ **Identify essential features based on your unique needs**

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 features that help you 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).

This matrix below illustrates this once difficult trade-off.



The vertical axis measures the level of fraud detection required to lower an organization's risk exposure. This goes beyond just fraud detection and includes a variety of risks including:

- Economic** – How much money was stolen
- Compliance** – Fines imposed for compliance lapses
- Reputational** – Impact on brand and consumer trust

Organizations that have a lot at stake such as banks, financial institutions and sharing economy sites will err on the side of fraud detection to ensure no bad actors slip through the cracks. Other companies are far more interested in optimizing conversion rates. For these organizations, it may be more important to onboard as many new users as possible with minimal friction. While no organization is comfortable with fraud, some may prioritize user conversions over fraud detection and may be willing to write off some level of fraud in the pursuit of more customers.

Finding the Right Balance

Ideally, a solution could offer both high levels of fraud detection with high conversion rates. But this requires incremental functionality. For example, starting the workflow with frictionless risk signals can enable more companies to add layers of identity assurance and fraud detection with no impact on the user experience. In order to do this, identity verification solutions must have the right combination of features and processes.

Your Verification Options

The table below provides a summary of the more popular online verification methods, each with their associated pros and cons.

Verification Method	Definition	Pros	Cons
Knowledge-Based Authentication (KBA)	Verifies customers by asking them to answer specific security questions in order to provide accurate authorization for online or digital activities.	• Well understood by users • Questions gathered over many years • Questions must be answered within defined time limit	• Easy to discover via social networking sites • Recent data breaches exposing personally identifiable information (PII) • Fraudsters can buy the information off the dark web • Often delivers a poor user experience • Does not rely on government-issued IDs and lacks a certain degree of authority
Two-Factor Authentication	An extra layer of security that requires not only a password and username, but also something that the user has on them, e.g., 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.	• Out-of-band authentication • Strong deterrent (fraudster must possess secondary token) • Near ubiquitous penetration of smartphones	• Vulnerable to key logging, SMS-spoofing, SIM swap fraud, man-in-the-middle and man-in-the-browser attacks • Bad customer experience if you lose one of your authentication factors • Can be slow and cumbersome • Users have to “have” their “something you have” all the time • Requires extra typing • Additional points of failure • Too easy for an inattentive user to approve an attacker’s transaction without knowing it • 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

Verification Method	Definition	Pros	Cons
Credit Bureaus	Many online identity verification systems call out to the big credit bureaus (such as Experian or GB Group), 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) • Fast results • No friction for end user	• 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 many false positives • Fraudsters increasingly have access to credit bureau data thanks to breaches • Does not rely on government-issued IDs and lacks a certain degree of authority • Data differs from bureau to bureau, leading to inconsistent results
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 • Analyze a variety of data from different sources to verify identity • Significantly reduce the number of manual reviews • Fast results • No friction for end user	• 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 and lacks a certain degree of authority
Online Identity Verification	Leverages automation to determine if a government-issued ID is authentic and belongs to the user. These solutions typically perform validity checks via a selfie to ensure that the person holding the ID is the same person shown in the ID photo.	• Uses a variety of AI, biometrics, machine learning and, if needed, human review • High verification assurance • Relies on valid government-issued ID and selfie to verify identity • KYC and AML compliance • API, SDK and web client implementations • Definitive, risk-based decision 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) • Additional verification information is typically not provided

Because of data breaches, knowledge-based authentication has become inadequate as a highly secure verification method. Similarly, credit bureau verification solutions aren't sufficient because of the inherent vulnerabilities with self-reported information. As a result, many companies are exploring 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 has become the logical successor to earlier approaches. By combining ID verification with selfie verification, emerging online identity verification solutions can ensure the person is who they say they are, is physically present and has possession of the ID.

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). Facial biometrics are especially important in determining that the person behind the biometric matches the one identified in the government-issued ID.

Key Verification Features

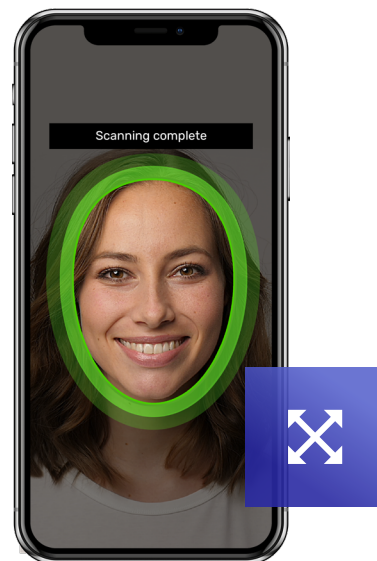
To help you better assess where a verification vendor sits on the fraud detection-conversion rate matrix, it's helpful to understand the underlying key features that can help improve fraud detection and user conversions.

Feature/Functionality	Fraud Detection	User Conversion
Liveness Detection	✓	✗
Fraud Database	✓	✗
Document Analytics	✓	✗
Expired IDs	✓	✗
Additional Documentation	✓	✗
Trend Spotting	✓	✗
Risk Signals	✓	✓
KYC and AML Compliance	✓	✓
Barcode & MRZ Scanning	✓	✓
Complete Answer	✓	✓
Human Review	✓	✓
Geographic Coverage	✗	✓
ID Version Support	✗	✓
Database of Valid IDs	✗	✓
Blur & Glare Detection	✗	✓

All too often, organizations evaluate vendors on a limited set of purchase criteria, such as price per verification and geographic scope. But there's a lot of nuance in what different solution providers bring to the table, and savvy buyers will go beyond the basics to find out about the solution's important features.

Liveness Detection

Increasingly, biometric facial recognition is being used to combat fraudsters who attempt to use static images, deepfakes, face morphs, face swaps and pre-recorded videos to fake their identity. With biometric facial recognition and liveness detection, better identity solutions can combat fraudsters who attempt to use these sophisticated means 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, organizations can significantly reduce fraud without impacting the customer experience.



Fraud Database

If an ID has been flagged as fraudulent (such as when it's been doctored or digitally manipulated), and someone attempts to use that ID again, modern solutions will capture this in their databases. Therefore, the more identity verification transactions a company processes, the more fraud they capture, the larger the database becomes and the greater their potential for catching fraud going forward. 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.

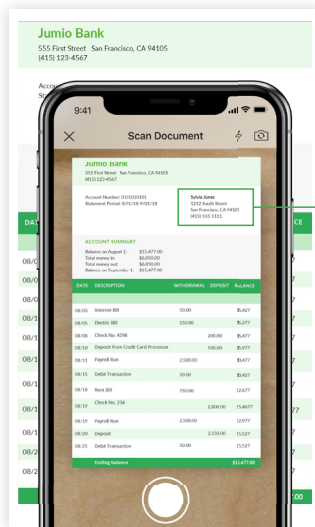
Document Analytics

Every government-issued identity document (ID) – whether it's a driver's license, identity card or passport – has a specification that defines the layout of the document, the relative position of specified fields, labels and images, font types, color, size, spacing and patterns. Every ID also contains a unique set of security features such as a ghost image, watermarks, holograms, microprint, chip and machine readable zones. Make sure your solution performs a variety of [AI-driven fraud checks](#) on these ID documents to ensure that the submitted ID conforms to these government templates and does not exhibit signs of fraudulent tampering, such as text and photo manipulation.



Expired IDs

Passport offices and many other agencies use a hole punch to mark an ID document as invalid, typically when you renew your ID. If an unexpired ID has a hole, it's been invalidated for another reason, such as when a license is suspended. Canceled and expired IDs should not be used for identification, and in fact, a canceled passport cannot be used for identification in any circumstance, including passport renewal. Unfortunately, many ID verification solutions cannot detect hole punches in IDs because of limitations in their technology. Jumio is one of the few digital identity vendors who can detect IDs with hole punches.



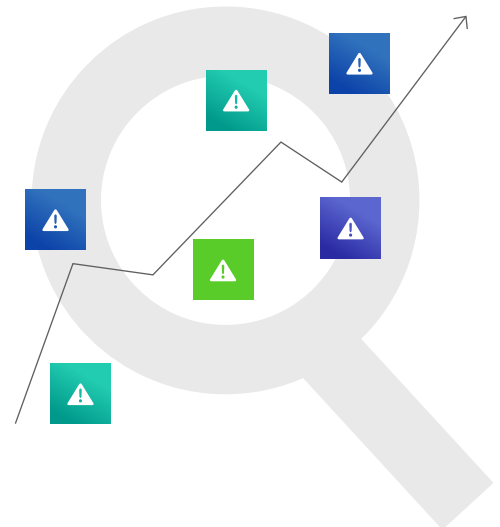
Sylvia Jones
1212 South Street
San Francisco, CA 94105
(415) 555-1111

Additional Documentation

When additional verification is required, such as proof of address, businesses need 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 online solutions that can extract data in less than ideal circumstances like scanning crumpled documents. Better solutions have the ability to extract Latin-based text (including English, French, Spanish and Italian) and non-Latin-based text (such as Chinese and Arabic characters) to include broader document support.

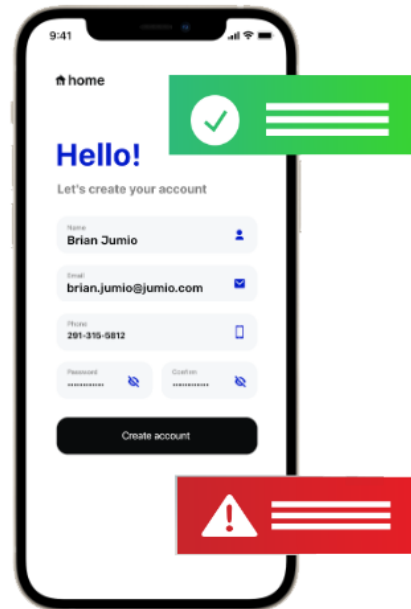
Trend Spotting

Let's say a fraud ring figures out how to doctor Nepalese driver's licenses. For many automated solutions, it can take weeks or months to update the code to recognize this new fraud trend. 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. The more transactions captured by an identity verification provider across many document types and geographies, the more business intelligence is 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.



Risk Signals

Risk signals provide a frictionless way to get extra assurance about a user's risk. For example, you can check the reputation of the user's device before they've entered any information, which is useful for stopping serial fraudsters who open multiple accounts in the same day from the same device. Similarly, you can check the age of their email address, their phone number's reputation, their IP address to make sure they're not in a high-risk location, and many more.



KYC and AML Compliance

When done via a smartphone or desktop webcam, identity verification presents an elegant solution for complying with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations without inconveniencing customers. Modern online identity verification solutions go beyond verifying the authenticity of a government-issued ID and also confirm the physical presence of the account holder. When the customer takes a selfie, the selfie image is compared instantly to that of the ID document, linking the ID to the owner in real time. And with an end-to-end platform like Jumio, you can also screen for sanctions, adverse media, politically exposed persons (PEPs) and more, allowing you to manage KYC and AML all in one place.

Barcode and MRZ Scanning

Most identity verification solutions can read the barcode on the backside of driver's licenses and the MRZs on passports. A user's first and last name, date of birth and contact details can quickly be extracted from these features. 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 extracted data matches the information on the front side of the ID and/or match the picture to the selfie taken?





Complete Answer

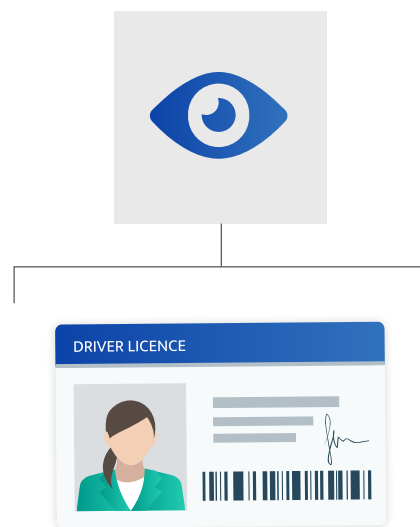
Most companies need a solution to accept or reject the user based on specific criteria that can be edited in real time as conditions change. More importantly, your verification solution should return additional information about why it rejected an ID (e.g., because the photo taken was a photo of a computer screen) or selfie (e.g., because the selfie is actually a photo cropped from the physical ID). This is essential for auditing purposes, both for accountability and for providing insights that can help you tune your configuration based on your risk tolerance.

It's also important to provide specific feedback to users as they go through the user journey. By telling them that the image is blurry or the light is too low and giving them a chance to try again, organizations vastly improve conversion rates and reduce friction for their users. With a simple "yes" or "no" solution, these good users would be rejected without being given the chance to course correct.

Unfortunately, many online solutions return only a score without clear explanations behind the 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. The best solutions maximize automation and provide human review as needed to verify the iffy transactions and improve overall verification accuracy.

Human Review

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 work with a vendor that has a large verification team with highly specialized, experienced and well-trained experts. You should also verify their service-level agreement to make sure they can complete the manual review in seconds or minutes, not hours or days.

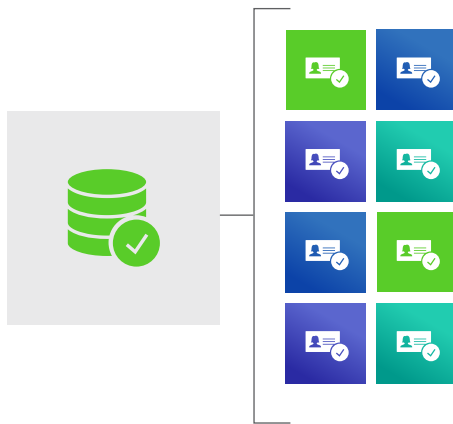


Geographic Coverage

Your provider must be able to 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 machine-readable zone (MRZ) on passports, but many of them cannot support other ID types such as ID cards.

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.

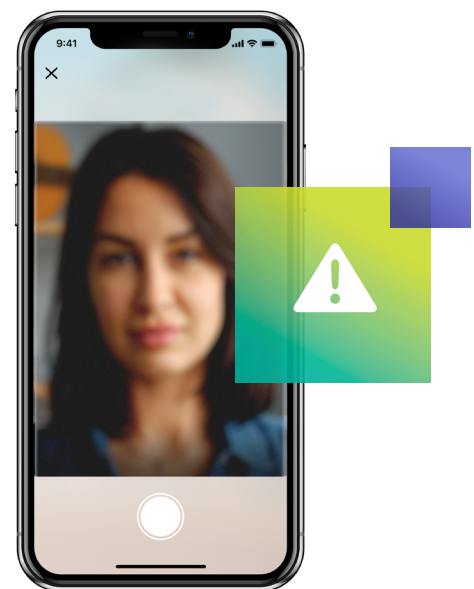


Database of Valid IDs

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. The opposite is also true when it comes to capturing legitimate and genuine government-issued IDs. If a verification solution has a large database of known, legitimate users, it can streamline the verification process, but only when paired with a proven face-matching solution.

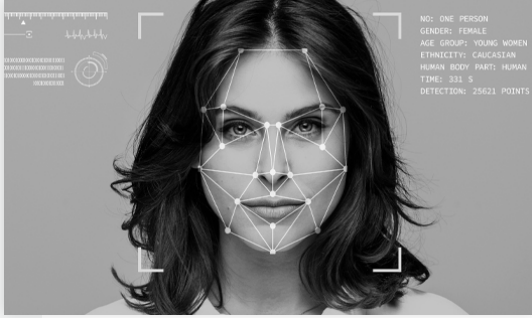
Blur and Glare Detection

Today's smartphone cameras provide crisp, high-resolution pictures. Unfortunately, this is not true for older phones or for photos captured with many webcams. If you allow users to capture images with a webcam, 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.



Next Steps

Now that you've got an understanding of the fundamental features you need for online identity verification, check out the following resources before you start comparing solutions:



Understand the underlying tech

You're going to hear a lot of technical terms, including artificial intelligence (AI), machine learning, algorithms, and omnichannel support. To get an understanding of what all these terms mean and how they'll impact your decision, check out [Metrics That Matter: How to Evaluate Identity Verification Technology](#).



Learn the best practices for a bake-off

To accurately test and compare identity verification solutions, there are some important best practices you'll need to put in place. For details, see [Identity Verification Best Practices for a Competitive Bake-Off](#).



Consider the true cost of each solution

To avoid being surprised by hidden costs, use our handy [Total Cost of Ownership](#) calculator to evaluate the true cost of each solution.

➡ [Contact us](#) to start a conversation about your specific use cases and how Jumio can help protect your business.

About Jumio

Jumio helps you to know and trust your customers online. From account opening to ongoing monitoring, the Jumio Platform provides AI-driven identity verification, risk signals and compliance solutions that help you accurately establish, maintain and reassert trust.

Leveraging powerful technology including automation, biometrics, AI/machine learning, liveness detection and no-code orchestration with hundreds of data sources, Jumio helps you fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including KYC and AML. Jumio has processed more than 1 billion transactions spanning over 200 countries and territories from real-time web and mobile transactions.

Based in Sunnyvale, California, Jumio operates globally with offices and representation in North America, Latin America, Europe, Asia Pacific and the Middle East and has been the recipient of numerous awards for innovation. Jumio is backed by Centana Growth Partners, Great Hill Partners and Millennium Technology Value Partners.

For more information, please visit jumio.com.

