Your buyer's guide to digital identity verification

How to meet the demands of your global business

Trulioo®

Executive summary

Digital identity verification plays a crucial role in protecting businesses and their customers from risk. And forward-thinking businesses are looking for identity verification solutions that also support their global growth and help them adapt to changing regulations and technologies.

This buyer's guide will help you navigate the complex identity verification landscape so you can make the best purchasing decision when it's time to invest. It describes the various methods of verification and authentication so that you can determine what will best meet your business needs. It also explains why an identity network, which enables a holistic approach to identity verification, is the most flexible and robust option for companies in high-risk and high-change environments.

Finally, this guide offers a comprehensive list of questions to ask that will help you evaluate identity verification providers before you buy.

Table of contents

Introduction:

The state of identity today

Every day, more activity is being conducted online. It's easier than ever to access education, financial services, marketplaces, healthcare and other essential services. As digital communications and transactions continue to gain worldwide adoption, our digital identity is at the crux of everything we do.

Unfortunately, technological progress also brings more threats from individuals who want to exploit these advances. In the hands of bad actors, the technology that makes our lives better — from business software to mobile devices to smartcards — also puts businesses and their customers at risk. New account fraud was up 13 percent in 2018,[1] money laundering is estimated at 2 to 5 percent of global GDP annually[2] and cybercrime is expected to cost the world $6 trillion annually beginning in 2021.[3]

These dangers have placed identity risk in the spotlight because they threaten two core human values: trust and privacy. As society combats the scourges of money laundering and identity theft, Anti-Money Laundering (AML), Know Your Customer (KYC) and privacy regulations have become more complex, stringent and numerous.

Businesses must also respond to competitive challenges and market shifts by expanding into new countries and launching new lines of business. This growth introduces the need to integrate more technology and comply with additional regulations, and the cycle continues.

This is the complex nature of business in the digital age. **Change is a constant, and processes for managing identity risk must be able to adapt to new conditions**. To survive and scale, companies must efficiently assess the various types of risks associated with digital identities when deciding who to do business with.

This guide is designed to help business leaders make sense of the growing world of digital identity verification solutions, understand different methods for assessing identity risk and determine the right solution for their needs.

[1] Rob Douglas, *Consumer Affairs*, "2020 Identity Theft Statistics," March 27, 2020.

[2] *United Nations*, "Money-Laundering and Globalization," March 2020.

[3] Steve Morgan, *Cybersecurity Ventures*, "2019 Official Annual Cybercrime Report," March 2020.

The business case for identity verification:

Ensuring compliance, preventing fraud, and increasing trust and safety

Let's explore what identity verification can help businesses accomplish today.

1. Achieve compliance

Concerned at the rise of fraud, money laundering and identity theft, regulators around the globe are rapidly implementing and expanding regulations aimed at curbing digital crime, including Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements.

These regulations can be confusing, and the fines for non-compliance can be crippling. In 2019, 58 anti-money laundering penalties[4] amounted to just over $8 billion in fines. In the U.S. alone, financial institutions have been charged $24 billion in fines in the past 11 years.[5]

Making sense of the dozens — or even hundreds — of regulations is a challenge, as is ensuring that your business remains compliant. Identity verification solutions can effectively and efficiently ensure that your business knows who your customers are every time, enabling you to meet all cross-border regulations and avoid non-compliance fines.

In 2019, **58** anti-money laundering penalties amounted to just over **$8 billion** in fines.

[4] Brian Monroe, *Association of Certified Financial Crime Specialists*, "Fincrime Briefing: AML fines in 2019 breach $8 billion, Treasury official pleads guilty to leaking, 2020 crypto compliance outlook, and more," January 14, 2020.

[5] Rupert Chamberlain, Jim McAveeney, Chetan Nair, Andrew Husband, Richard Robinson, *KPMG*, "Combating financial crime," March 2019.

2. Prevent fraud

Despite global attempts to reduce online identity theft, cyberattacks are more ambitious, new account fraud is up and account takeovers have risen 79 percent.[6] Fraud represents a significant risk to operations, both in terms of financial consequences and reputational damage.

When an applicant requests an account, identity verification processes can flag potential fraudsters before any damage is done. Anomalies in identity information, such as out-of-date information or mismatches in data, can quickly reveal issues for further examination. By cross-referencing multiple data points and data sources for identity checks, you create an even higher barrier for a fraudster to overcome.

Depending on the risk mitigation strategy, further identity authentication measures can also be deployed. For example, requiring proof of possession of an identity document or mobile device associated with the account holder makes it harder for the fraudster to take over an account.

Proper implementation of account opening best practices can reveal bad actors. Whether they're attempting to open an account despite being a known entity, or they're pretending to be someone they aren't, a layered approach to identity verification helps prevent fraud.

3. Build trust and ensure safety

The world is going digital; according to the International Data Corporation, 60 percent of the world's GDP will be digitized by 2022.[7] The ability for digital identity verification to deliver safety, security and trust is a key enabler of the new world economy.

New account fraud is up and account takeovers have risen **79 percent.**

New forms of interactions and transactions are changing the way we relate and do business. The marketplace economy, where people share resources with other people, offers new opportunities and challenges. A fundamental requirement for a successful online marketplace is the safety of the participants; each party needs to be able to trust the other, both on a physical safety level and on a transactional level. Properly vetting participants, including verifying their identities, increases peace of mind and security for everyone in the marketplace.

As the Financial Action Task Force (FATF) states, digital identity holds "great promise for improving the trustworthiness, security, privacy and convenience of identifying natural persons."[8] By digitizing the identity process and implementing strong identity verification solutions, businesses can lower costs and risk, improve their ability to expand into new markets, and better build trust with customers, employees, suppliers, third parties and all their connections.

[6] Javelin Strategy, *2019 Identity Fraud Study*, March 2019.

[7] IDC, *FutureScape Report*, October 2018.

[8] FATF, *Guidance on Digital Identity*, 2020.

The value of a risk-based approach

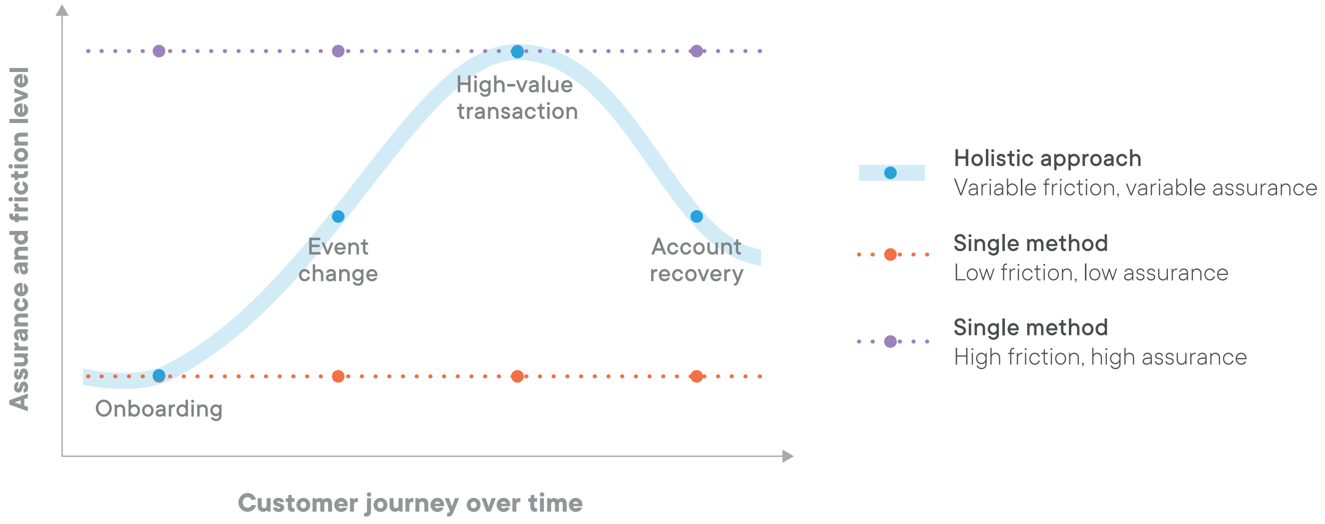
Focus on the goal first, then the method

A risk-based approach to trust and safety, compliance, and fraud prevention does not dictate a particular method of identity verification, for several reasons. First, because technology, regulations and business models are always changing, a verification process built around a single fixed method may not be able to adapt to new types of fraud or new legal requirements. Second, a single method that only verifies one facet of identity doesn't always go far enough in reducing risk. It's easier for a bad actor to get past the verification process if it only checks an ID document, for example, but doesn't verify the personally identifiable information (PII) on that document or authenticate the user with biometrics.

Instead, a risk-based approach is oriented around managing risk by matching the verification process to the risk level. It involves creating custom verification workflows based on each type of customer and transaction. This flexible approach provides a much higher confidence level of identity proofing because it allows for cross-checking different facets of identity when the risk profile calls for it.

A risk-based approach is key to balancing risk mitigation with user experience.

Historically, identity verification was a compromise: it either came with high levels of fraud detection but significant friction, or it came with minimal friction but low levels of fraud detection.



▲ **Figure 1.** With a single identity verification method, businesses have to make a choice:

- Low friction, low assurance, or
- High friction, high assurance

With a holistic approach, businesses can customize the verification workflow to fit the risk level and keep friction to a minimum.

Sacrificing convenience for security — or security for convenience — no longer works for users or businesses. Abandonment rates skyrocket when customers feel that opening an account or onboarding takes too long. The rise of digital fraud and non-compliance fines means that sacrificing risk mitigation can be too costly for businesses. RegTech solutions for identity verification have developed to address that trade-off and solve for both customer experience and risk.

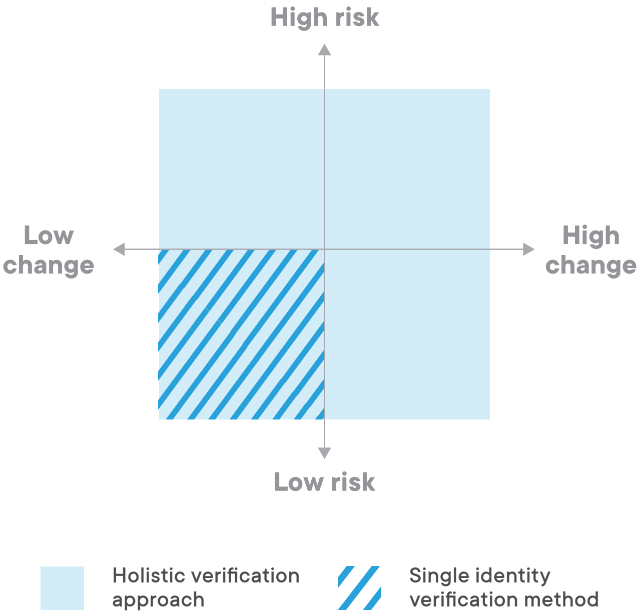
As the first touchpoint customers have with a business, the onboarding process should be as frictionless and secure as possible. Businesses must view quality onboarding as a core product in and of itself.

If successful, this first step along the customer journey can drive long-term loyalty, repeat business and revenue conversion, all while maintaining compliance and security amid ever-changing regulations.

A digital identity network is the ideal for deploying a risk-based approach to identity verification.

Each business is unique. Some are local, others are global. Some have users largely interacting with the business via mobile phones, while other businesses see engagement mostly on desktops. For some, the majority of users are located in developing regions where traditional forms of identification are rare. For others, the typical user has no shortage of identity documents.

A digital identity network, which offers multiple verification methods across many markets, has the flexibility to meet those unique business needs. It can cover any and all regions a business operates in, today and in the future.


High risk
Low change
High change
Low risk
Holistic verification approach
Single identity verification method

◀ **Figure 2.** A single identity verification method is enough to handle low risk transactions in low change environments. However, if the risk increases or if the environment changes because of regulations, technology or growth, only a holistic verification approach can help a business adapt to the new situation by changing or adding to the identity verification method.

An identity network lets you choose and combine verification methods that are best for your risk profile. Businesses can progressively build trust with customers based on the nature of the relationship and the context of the exchange, without adding too much friction to the onboarding process.

Varying risk profiles

Accounting for use cases, industries and geographical markets

The risk involved with a transaction depends on several factors:

- The value of what’s being exchanged. Is it a low-value asset like a free account or a large sum of money?
- The nature of the relationship. Is it a new relationship or a long-standing relationship with a high degree of trust?
- The threat posed by bad actors taking advantage of the transaction. Would it be a small limited loss? Or could it result in fines and reputational damage?

Financial institutions and gambling operations have different risk profiles than eCommerce and retail stores. Businesses that are regulated must account for the risk of fines and penalties. But any business that is exposed as untrustworthy, whether regulated or not, risks reputational damage and loss of customers.

Risk profiles also vary between countries, because of the relative ease or difficulty in verifying identities from that country, because of differences in regional regulations, and because of the level of transparency.

Identity risk profiles are also different within an individual business, along the entire customer journey. For example, consider an online casino. When a player opens a gambling account with a small sum, the casino only requires proof of age, because the transaction value is low. However, if the player starts gambling with amounts over $1000, the risk profile changes, and the casino performs KYC to comply with regulations. If the amounts go over $10,000, the risk profile changes again, because the threat of fraud has increased, and the casino takes additional steps to protect against loss.

Given all the factors that can lead to varying risk profiles for a company, a risk-based approach for identity verification provides the most flexibility for handling different risk profiles efficiently.

The many facets of identity:

Physical and digital attributes that identify an individual or business

Before getting into the mechanics of identity verification, it’s important to understand the multifaceted nature of identity. A single person or organization has one identity, but that identity has many different attributes, both physical and digital. Here’s how it breaks down.

Identity data

There are hundreds of data points that together form the full picture of who you are. These data points are called personally identifiable information (PII) when they can be used to identify a specific person (think: name, date of birth, phone number, IP address, email address, or ID number).

Businesses are likewise identified by data points, including business name, business address, and business registration number. Businesses also have owners who can be identified with personal data.

ID documents

Identity documents such as driver’s licenses, passports, residence permits and identity cards are a physical representation of identity. They can also store PII digitally, in machine-readable zones or chips, and carry photos of the bearer’s face.

Businesses have documents of record as well, such as annual accounts, articles of association and register reports.

Verified accounts

When account owners are subjected to an identity verification process to open a bank, utility and mobile phone account, those accounts become another attribute of an individual or business identity.

Devices

Mobile phones and hardware authentication devices such as security keys can be tied to a particular identity. Possession of the device is linked to the identity of the device owner.

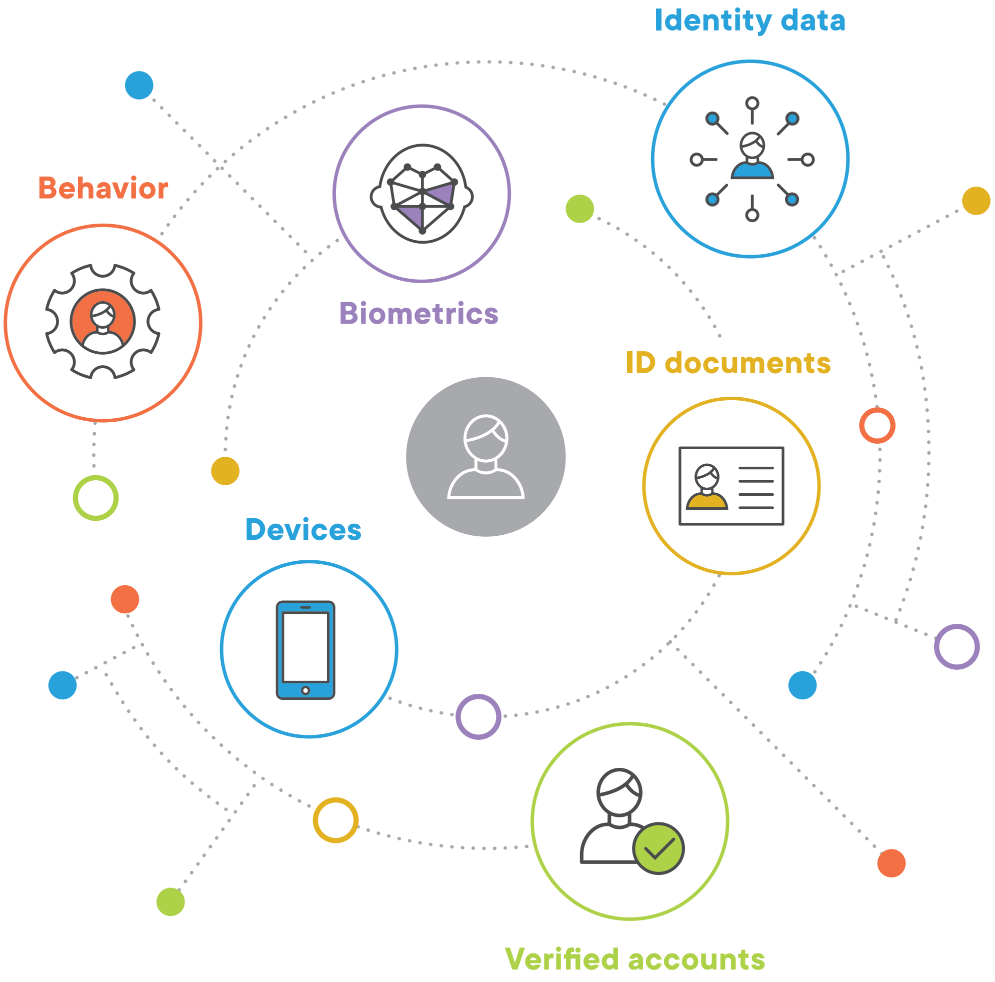
Behavior

From location and frequency data to news mentions and crime records, an individual or business’ activity in the world is tied to their identity. The wealth of digital activities that are part of everyday life create patterns that can be traced to a particular person or organization.

Biometrics

An individual’s unique physical identity includes their face, fingerprints, palm prints, and retinas. These biometrics can be scanned and stored digitally in databases or on mobile devices or smartcards.

Any or all of these facets of identity (data, ID documents, verified accounts, devices, behavior and biometrics) can be used to assess the risk associated with that personal or business identity.



▲ **Figure 3.** Identity has many physical and digital attributes. The more attributes that are verified, the higher the degree of assurance that you have identified the individual correctly. An identity network lets you customize which identity attributes are verified when, rather than limiting you to verifying one or two fixed attributes.

Making sense of identity verification methods:

Examining the numerous verification methods on the market

Given all of these factors — constant change in the operating environment, the varying risk of transactions and the multifaceted nature of identity — assessing identity risk can be a complex undertaking. Many people in developing parts of the world lack traditional forms of identity records or documentation, making verification more challenging. When the traditional in-person process of matching a person's face to an ID card is translated to the digital world, it needs to handle a wide array of ID documents belonging to users from every corner of the world. What's more, the rapid rise of mobile and smartphones has added new factors that global businesses must accommodate.

When assessing the risk associated with a specific identity, whether that's an individual or a business, there are a number of questions that can be posed:

- **Is this a real identity?** Or has it been fabricated? Determining whether an identity is real is known as *identity verification*.
- **Does this identity belong to the person claiming it?** Or has it been stolen? Determining whether a person is who they say they are is known as *identity authentication*.
- **Has this identity been flagged as high risk?** Have they committed a crime or do they hold a position that makes them susceptible to corruption? Is the identity associated with previous fraud attempts? Determining whether a person has been flagged is called *risk screening*.

Numerous digital methods have emerged to help businesses answer these questions, in order to assess identity risk and comply with regulations.

The table on the next page details the most widely used methods for assessing identity risk.

Goal	Identity Attribute	Description	Methodology
Verification	Data	Checks personally identifiable information or business vitals against independent, third-party data sources to ensure that an individual or business is real and not a false identity attempting to commit fraud.	For individuals, checks a person's PII (name, date of birth, address, phone number, and more) against trusted global data sources (such as credit bureaus, electoral rolls, national IDs) to make sure that person exists. The data could be submitted by the person or extracted from their identity document. For businesses, checks a business name, business address and business registration number against official registers. Also verifies the personal identity data of Ultimate Beneficial Owners (UBOs).
Verification	ID Documents	Collects and analyzes official identity documents. *Note that the data on the identity document must also be verified to ensure that the person exists.*	For individuals, captures images from a person's identity document (such as driver's license, passport, ID card or resident permit) with a mobile device or high-quality webcam, and assesses whether the document is valid (not expired, manipulated or forged). For businesses, downloads documents from official registers, such as annual accounts and articles of association.
Verification	Verified accounts	Confirms that a person or business exists because they have access to a verified account such as a bank account.	Requires the account holder to enter their account credentials (user ID and password or account number) to prove that they own the account.
Authentication	Biometrics	Compares a person's biometrics, such as face, fingerprint or retina, to a trusted record of identity to ensure that they are the true owner of that identity.	Users are prompted to take a selfie photo. Facial recognition technology (such as machine learning, artificial intelligence and liveness detection) compares the selfie to the photo on the ID document.

Goal	Identity Attribute	Description	Methodology
Authentication	Device	Confirms that a person is who they claim to be because they have possession of a device belonging to that person.	Sends an SMS text message to a person's mobile phone containing a code or link. Clicking the link or entering the code confirms that they have the mobile phone connected to the identity they're claiming.
Risk screening	Behavior	Checks identities against global risk data sources (sanction lists, law enforcement lists, governing regulatory bodies, fraud data, self-exclusion lists) to ensure that an individual is not high risk.	For individuals, checks global risk data sources to see if the person's name is listed. For businesses, screens the business entity and the names of Ultimate Beneficial Owners (UBOs) against global risk data sources.

Identity verification checklist:

What to look for when evaluating

The company behind the solution is as important as the technology itself. One World Identity's 2019 Identity Industry Landscape[9] found that the number of identity companies has more than quadrupled since 2017, going from 500 companies to over 2,000. Many of these companies state that they offer best-in-class identity verification solutions; however, often businesses don't have the time or expertise required to properly evaluate them.

To aid businesses when evaluating countless data sources, verification processes and vendors, Gartner[10] recommends that businesses:

- "Perform an inventory of their current identity proofing methods ...
- Include the cost of poor customer experience when evaluating ...
- Prioritize the detection of identity-related attacks at all facets of customer interaction ...
- Ensure the identity proofing strategy ties into a broader risk management framework ...
- Evaluate the use of an identity hub to enable the orchestration and testing of multiple solutions as the need arises."

[9] *One World Identity*, "2019 Identity Landscape," 2019.

[10] Akif Khan, Jonathan Care, *Gartner*, "Market Guide for Identity Proofing and Corroboration," September 30, 2019.

Evaluating identity verification providers: Questions to ask before you buy

Trulioo has spent nearly a decade testing and integrating hundreds of identity data sources and services, which enabled us to build a robust identity network. We have acquired in-depth knowledge of global identity verification, and we share our insights and expertise to support our clients. We have created a helpful checklist of features and criteria when evaluating an identity verification provider. It reflects a wide range of business needs, regulatory environments and customer expectations.

	Vendor 1	Vendor 2	Vendor 3
Which types of verification are offered?			
What user information does your business need to verify? Does the solution offer these options? ▪ Identity verification (IDV) for age, address, name, national ID number, and more ▪ ID document verification ▪ Account verification ▪ Biometric authentication (selfie, live detection) ▪ Device authentication ▪ Business verification ▪ AML watchlist checks What verification needs does your business require (KYC, CDD, AML, KYB)? How are these verification options implemented into your workflow? Can they be combined into a single solution? How does the solution prevent fraud and illegal activity from passing the verification gate?			

	Vendor 1	Vendor 2	Vendor 3
Dynamic routing for optimized verifications and user experience			
Does each data source or service have built-in redundancy? Can you optimize verification workflows to route to a different data source or identity service (for example, ID document verification) to help increase acceptance rates?			
Multiple integration options			
How does the solution integrate into your current workflows? Are there multiple options for how to integrate the solution that suits your business needs best? ▪ API ▪ Web portal access ▪ Low-code front-end developer tool Does the solution include an image capture SDK for document verification and selfie/liveness checks? Does the solution require you to integrate one image capture SDK or several? Does the provider offer batch verification for testing results and running verifications outside the automated workflow?			

	Vendor 1	Vendor 2	Vendor 3
Multiple integration options (continued)			
How easy is it for you to deploy their solution? What does the integration, testing and launch process look like? How much time and developer effort does it take to integrate with an identity verification solution to get the coverage and flexibility you need? Will you need to engage with multiple data vendors and identity service vendors to address all of your requirements, or just one? Will you need to integrate one API or many? Will you need to build one data capture form for the world or one for each country? Are the data fields normalized?			
Timing			
Once the agreement is signed, how long is the integration process before you can begin verifying customers? Is the timing the same for one market vs 20? Does this solution offer real-time verification? Does it offer waterfall options for manual checks?			

	Vendor 1	Vendor 2	Vendor 3
Analytics			
Does the solution offer in-depth analysis on performance and verification rates? Does the solution provide recommendations on country-specific inputs? Does the solution have a team of data scientists and analysts who help detect fraud? What is the process for flagging key issues that may affect your business, such as suspicious transactions?			
Account management			
Does the provider offer a dedicated account manager to support audits and reporting? Does the provider offer a dedicated account manager to provide optimization expertise? Do they offer a dedicated implementation specialist or a technical contact to ensure proper integration and setup?			

	Vendor 1	Vendor 2	Vendor 3
Expertise			
Does the provider have expertise and experience in your specific industry? Does the provider understand your business needs and have a strong reputation for meeting them with other businesses with similar needs? Does the provider continuously expand to new countries and increase coverage by procuring new data source partnerships to integrate into its solution? Does the provider allow you to build custom configurations per country based on local risk and compliance requirements? Does the provider allow you to build custom verification workflows that combine and layer various identity verification and authentication methods?			
Privacy and security			
What compliance standards does the provider follow? How are regular checks performed for compliance? Who performs these checks? How is user data handled and deleted? What certification does the provider have for their solutions? Do they adhere to any ISO or other standards?			

Evaluating identity verification methods

For verifying identity data:

	Vendor 1	Vendor 2	Vendor 3
Data sources and its origins			
How many types of data sources does a solution offer for identity, age and address verification? Do those sources include mobile network operators (MNOs), public records, credit bureaus, resident files, business registries, banking and financial sources, and government sources? What data sources are available for fraud detection? What data sources are available for AML? How often are the data sources updated? What is the response time of each data source? How is the level of coverage determined for each data partner? How do these data sources collect and store consumer information? Do they have consumer consent or any restrictions on its use? What criteria are used to procure and integrate data partners?			
Customized rulesets			
Can you customize verification rules based on your risk assessment and needs? Can you customize for AML requirements based on countries to give the highest number of customer verifications possible?			

For all verification methods:

	Vendor 1	Vendor 2	Vendor 3
Breadth of coverage by country/market			
How many countries and markets does the solution cover? Are there reputable and secure data points in each of these markets? What is the percentage of population coverage in these countries or markets? What types of data sources does the provider have access to within each country? How many secure and unique data sources can you access to verify both personal and business identities? Can the provider compare different data sources within a country to get the best match rate? Does the provider have the best data source coverage to accurately verify users in all of your markets? How many types of ID documents can the solution analyze and verify? Can it source unique ID documents from various countries and check for authenticity?			
Transparency of verification results			
Does the solution provide a score? If so, does the identity verification provider offer transparency on how the score is obtained? Does the solution provide a breakdown of where and which data touchpoints were used?			

Conclusion

Fostering trust, privacy and safety through identity verification

In a world where identities are compromised daily, nothing is more critical than fostering a climate of trust, privacy and safety online.

As this buyer's guide has shown, businesses are not alone in this fight; a global identity verification market has matured to help businesses weed out the bad actors and bring in only the good customers.

Sifting through this market is not simple or straightforward. The true effectiveness of an identity verification solution is only achieved through real-world testing, implementation and refinement.

Like identity verification providers, no two consumers are the same or static; each has different expectations, access to technologies and attitudes towards privacy. Consumers' profiles will continue to evolve as the world changes rapidly around them, and they need a provider that can keep pace with these changes.

As we laid out in this buyer's guide, it is important to start with a clear understanding of your business' current and potential future needs. With this context in mind, exploring and comparing the available options will allow you to make informed purchasing decisions. With increasing fraud and resulting regulation, the price of failing to do so is costlier than ever before. But the right solution can not only avoid these problems, it can also ensure customer privacy and trust and help you stay ahead of the competition in an increasingly digitized world.

About Trulioo

Trulioo is a global identity and business verification company that provides secure access to reliable, independent and trusted data sources worldwide to instantly verify consumers and business entities online. GlobalGateway, the Trulioo identity verification marketplace, helps organizations comply with Anti-Money Laundering (AML) and Customer Due Diligence (CDD) requirements by automating Know Your Customer (KYC) and Know Your Business (KYB) workflows. Trulioo supports global clients to instantly verify 5 billion people and 330 million business entities in over 195 countries — all through a single API integration. Named as a CNBC Disruptor 50 Company, the Trulioo mission is to solve global problems associated with verifying identities by powering fraud prevention and compliance systems for customers worldwide in an effort to increase trust and safety online.

For more information visit **trulioo.com**.