The Ultimate Guide to

Trust & Safety in the Sharing Economy

jumio

Introduction

Global economies have experienced a massive shift over the last decade as the sharing economy has taken root. The sharing economy — loosely defined as a peer-to-peer exchange of goods and services that is facilitated by an online platform — is evolving due to technological innovations, economic factors, changing demographics, environmental concerns and even a resurgence of the concept of community.

Lodging, transportation and consumer goods companies like Airbnb, Uber and eBay were among the first brands on the scene, but the sharing economy is rapidly expanding into new industries, including grocery delivery (Instacart), professional services (Fiverr) and even healthcare (Doctor on Demand).

By 2028, the sharing industry is expected to skyrocket to $794 billion, an increase of 5,571 percent since it first emerged in 2014 as a $14 billion industry.

With such a disruptive yet lucrative business model, investments in the sharing economy have seen a corresponding uptick. According to the BCG Henderson Group, 85 sharing companies raised $130 million in venture capital in 2010. In September 2023, Tracxn reported total funding reached $124 billion across 2,516 companies. This growth is being fueled by convenience, cost, and the principles of trust and safety.

Trust is a prerequisite for the sharing economy to thrive — the expectation that all parties are who they say they are and are operating in good faith. When college students rent rooms over summer break through Roomi, we trust that their roommates have been vetted. When we call for an Uber after a night of drinks, we trust that our driver will get us home safely.

Consumers in the sharing economy trust that the company has done due diligence in verifying the identities of its providers (e.g., drivers, delivery people, hosts, freelancers) and that their services are trustworthy and safe. Likewise, providers have faith that new users have passed some sort of identity verification before being accepted onto the sharing platform.

When this trust is broken — as we've seen on Craigslist, GoFundMe and elsewhere — it's the company that is held responsible. Once broken, trust cannot be easily repaired.

Consumers Support Identity Verification

The Jumio 2023 Online Identity Study found that 70% of global consumers would be willing to spend more time on identity verification when using a sharing economy site.

Source: 2023 Online Identity Consumer Study Jumio Global Research

Importance of Biometric Identity Verification in the Sharing Economy

To what extent do you feel biometric verification is needed for sharing economy services?

Source: 2023 Jumio Online Identity Study
Net figures, with global figures representing findings for four polled markets.

Fostering a relationship of trust and an environment of safety goes well beyond keeping fraudsters out. It's become a brand imperative.

Trust can be made — and broken — across a spectrum of experiences, from unfair reviews to data breaches to a poor user experience. But safety, and therefore trust, can be earned and cultivated through sound policies and practices.

In this Ultimate Guide to Trust and Safety in the Sharing Economy, we will provide an overview of the sharing economy, including the factors to consider as you seek to build trust and safety through an online identity verification program. You will learn about:

- **The Sharing Economy at a Glance**
- **The State of Trust and Safety in the Sharing Economy**
- **How the Industry is Working to Instill Trust and Safety**
- **Challenges with Online Identity Verification**
- **Five Elements of a Successful Solution**
- **How Jumio Can Help**

The Sharing Economy at a Glance

In the last decade, companies like Airbnb and Uber have carved out an entirely new niche in the marketplace, called the "sharing economy." Let's take a look at this rapidly evolving industry.

An Evolving Definition

While there is no single definition for the sharing economy, it originally emphasized the sharing of under-utilized assets (e.g., an empty vacation home) between the owners of those assets and those seeking to use them (e.g., a family on vacation). In nearly all cases, the exchange is made possible through an online platform, or app.

Also referred to as the collaborative, gig, peer or trust economy, the sharing economy is constantly evolving. It now encompasses a range of economic transactions and platforms, including:

Collaborative
Matching people with goods or services they need to the people or marketplaces that have them. (Etsy, OfferUp)

Peer-to-Peer Lending
Enabling individuals to lend money to one another directly, usually at attractive rates. (Kiva, LendingClub)

Freelancing
Pairing remote freelance workers with employers who need temporary or part-time help. (99designs, Fiverr)

Crowdfunding
Bringing together entrepreneurs, inventors or other people in need of funding with investors and donors. (GoFundMe, Kickstarter)

Co-working Platforms
Providing shared office, retail or other space to enable solopreneurs access to affordable business space and services. (WeWork, Coworker)

"Sharing saves people time, money and aggravation. But what really greases the wheels of this fast-growing economy is trust."

- Forbes

The Generational Gap

To what extent do you feel biometric verification is needed for sharing economy services?

Source: 2023 Jumio Online Identity Study
Net figures, global averages

Younger adults want verification before trust in the sharing economy.

Notable Players

Sharing providers in the transportation (CityScoot, Zipcar, DidDi), retail goods (Rent the Runway, Etsy) and hospitality (CouchSurfing, VRBO, SabbaticalHomes) opened the floodgates to many other peer-to-peer services.

Two notable additions in recent years have been crowdsourcing sites (Indiegogo, Kickstarter) and "gig" or freelance opportunities (e.g., software/IT professionals, accountants, graphic designers, construction workers and healthcare aides).

Looking ahead, we can expect to see continued growth in the healthcare (Cohealo, HD), delivery (Instacart, Doordash) and professional services (Upwork, TaskRabbit) markets. We're also seeing innovation in some unexpected places, like land sharing (Fresh Start), clothing rental (Tulerie, Pickle), space sharing (StoreFront, Popuppens), equipment sharing (EquipmentShare, PreferRent) and parking space sharing (Neighbor, BestParking).

In 2021, Pew Research Center found that 16% of U.S. adults have earned money through an online gig platform, and **30% said it was their primary job.**

What's Driving the Demand?

A culmination of technological, economic and cultural trends have contributed to the growth of the sharing economy.

Convenience

The access and convenience of doing business online — from finding a babysitter to booking a handyman for that home repair — makes our lives easier. We can do transactions over our smartphones, find the best pricing, and access curated resources we might not otherwise know about. It's what the younger, digitally savvy consumer has grown up with and expects.

Sharing platforms are causing major disruption in hotel, transportation and consumer goods industries, forcing traditional, brick-and-mortar brands to change or get left behind. They're also elevating the importance of online reputations, creating a more level playing field between longtime brands and new businesses.

Economic Value

Whether it's due to financial circumstances or a merely a lifestyle choice, many young adults choose not to purchase expensive items like homes and cars. According to Bankrate, "Gen Z is the first generation to grow up with access to private transportation in the palm of their hands. With ridesharing, bike-sharing and electric scooter options, many Gen Zers don't need to own a car and save money using app-based transportation options instead."

For those with demonstrated hardships, sharing platforms for everything from farm equipment (Trringo, Hello Tractor) to education (Kytabu) open up new possibilities.

Cultural Shifts

Though economic factors are the primary driver fueling growth, personal values are also contributing to changing economic patterns. One reason is the sharing economy has been shown to be better for the environment, in part because it reduces waste and cuts carbon emissions.

A return to a sense of community and belonging has also prompted many users to engage in sharing services like Kiva, which provides small, crowdfunded loans to individuals and small businesses across the globe.

Flexibility

Renting and sharing allow people to live the lives they want without spending beyond their means. For millennials, that means they can travel frequently, work remotely and have the freedom to explore different parts of the world. For everyday workers, it means having the flexibility to choose when, where and how often they work. And for families, it means destination vacations are suddenly within financial reach.

The Linchpin to Success: Trust & Safety

If convenience and affordability are the engines of the sharing economy, trust is the fuel that keeps the engines running.

Trust is that magic ingredient that allows us to feel safe getting into the car of a complete stranger or reassured that when we show up to a stranger's home, there will be a clean room waiting for us.

At the heart of trust is the concept of safety. Can I be confident that the person I'm dealing with is who they say they are, will deliver on their promised goods or services, and will operate in good faith? In other words, will this transaction be safe — financially, physically and emotionally?

Ratings systems and 24/7 assistance boost user confidence, and one report indicates that the sharing economy even helps reduce crime. But all of this depends on knowing the identity of the other party.

Where identity verification comes in:

A critical component of building trust in the sharing economy is verifying the real-world identities of stakeholders. And since trust is a two-way street, that can often mean verifying both the providers and the users of the service.

For instance, Uber and its community of drivers and ride sharers want to know that you are, indeed, who you say you are. Likewise, when you book a ride, you want to know that the identity of the driver has also been verified.

In the next section of this guide, you'll learn more about the role of online identity verification in promoting trust and safety.

The State of Trust & Safety in the Sharing Economy

Trust is, to a degree, about perception, however its foundational element is safety. From the moment a user signs on to your service, they are forming opinions about how safe they feel, and therefore how much they trust you. Your ongoing interactions with them have the capacity to strengthen or weaken that trust.

In the sharing economy, the concept of trust and safety goes well beyond the traditional emphasis on data breaches, fraud or identity theft. The threads that weave the blanket of trust are much more nuanced. Often, they don't involve the exchange of money or goods at all.

Unlike traditional IT security, trust and safety tend to be policy- and practice-driven. The company decides what the potential threats to trust are, creates a set of policies to minimize those threats, and fosters a culture within the organization to support those themes.

Only when both users and providers feel confident that your organization has put measures in place to keep them physically, financially and mentally secure, will they trust your platform.

How Trust Can Be Damaged

Data breaches, identify theft, credit card fraud

Unfair or aggressively negative reviews

Malicious bots used to disrupt forums, increase traffic, pose as real people, etc.

Online fraud and account takeovers

Misrepresentation of goods or services

Violent or discriminatory behavior by the provider or user

Catfishing or dating fraud

Slow or non-existent customer service

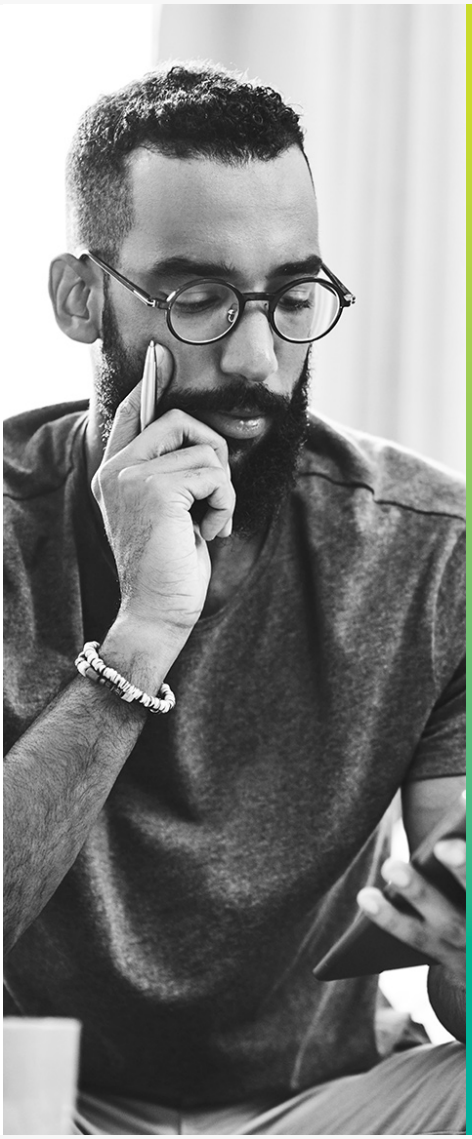
Building a trusted brand where users feel safe and secure is crucial. The leading sharing brands already have Trust & Safety initiatives in place. Airbnb, for example, outlines how they foster safety for providers and users across these areas: risk scoring, background checks and watchlists, host preparedness training, secure transactions, account protection, scam prevention and secure messaging.

Upwork's Trust & Safety initiative focuses on the relationship between the employer and the freelance worker, including pre-assignment vetting, fair review policies and pricing. They also have a section dedicated to staying secure online.

Creating an effective trust management ecosystem is challenging. It starts with the core building block of information security, but quickly expands to include credentials verification and management, and beyond.

Consumer Concerns

The astronomical growth of sharing services hasn't happened without its share of growing pains, and consumers aren't shy about communicating their concerns.



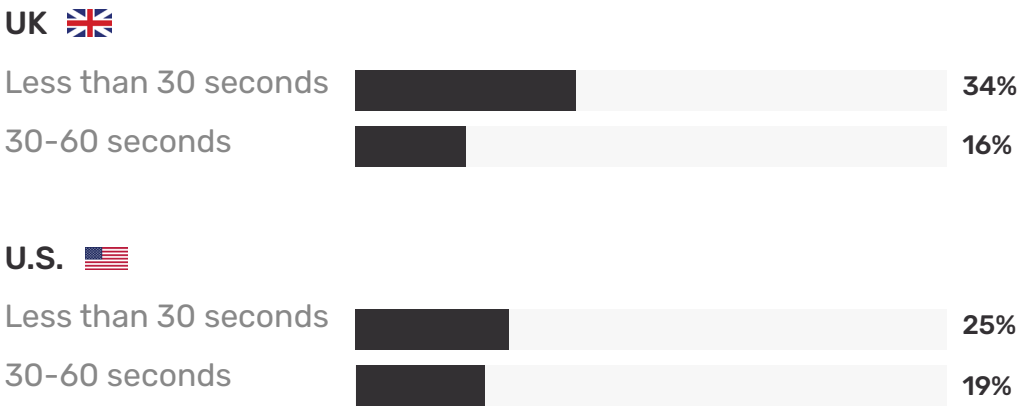
The Sign-up Process

Digital transformation has made the account opening process much faster and more convenient. Rather than visiting a branch and filling out paperwork by hand, we can easily open an account from our laptops and even our phones.

Despite the added convenience, consumers have little patience with a slow or cumbersome onboarding experience and expect the sign-up process to take a minute or less.

Users Want a Quick Sign-up Process

How much time would you be willing to spend to complete your online identity verification when creating a new account for an online sharing service?



Source: 2018 Jumio Global Consumer Trust and Safety Survey

The ability to join a service needs to be as seamless and pain-free as possible. Users will abandon processes that create a lot of friction, whether it's the time necessary to complete the steps or the volume of information required to finish the application.

Case in point: Signicat did a study in 2022 and found that

68 percent of banking account applications were abandoned

due to a long or complicated enrollment process. Users want to sign up online, and they want the process to be fast and easy.

Volume and Use of Personal Data

There are multiple levels of data users provide when they sign up. There's basic profile information like usernames and passwords. Then there is the Personally Identifiable Information (PII) normally required to set up and verify an account, including email, address, government ID number (e.g., Social Security number) and photo ID. Finally, there's the data that's generated once the user engages with the service (e.g., GPS location, number and types of transactions).

The public has become simultaneously wary and desensitized by the amount of and frequency with which they provide data to third parties. They are willing to share data if the purpose and use of that data is made clear up front, but they also expect companies to have measures in place to protect their data once it's been collected.

Background Checks/Verification

While there is some reluctance to provide too much personal information, users still want the sharing service to verify the identities of others on the platform. They want to feel confident that people are who they say they are, that reviews are legitimate, that their physical safety won't be endangered and that they will remain financially unscathed.

The importance of verification extends beyond the application phase. Consumers also want assurances that there will be ongoing monitoring of stakeholders, or at least a periodic re-verification/secure authentication that the people using the service are indeed the account holders.

Identity Verification Is Important to Users

How important is it to you that the online sharing services you use incorporate an identity verification process for all new users?

UK

Very or Somewhat Important

58%

U.S.

Very or Somewhat Important

71%

Source: 2018 Jumio Global Consumer Trust and Safety Survey

Bot Scams

Any site that draws high traffic — particularly if it's from less-than-savvy internet users, like dating websites — is ripe for scammers to use bots. There's usually a real person behind the scam, but they use a bot to sign up for the service and target their prey (e.g., women over 50). There are various methods for luring victims, such as appealing to their romantic instincts (e.g., I'm a widowed military veteran seeking love) or those that respond to an inquiry with an automated message (e.g., it's so great to hear from you, let's become Facebook friends). The scam continues to progress until the victim is in a fully compromised situation, is hacked or has been conned into sending money to the scammer.

Verification systems not only help with rooting out bad actors in real life — they can also prevent bots.

Practicality and Ease of Use

Once verified, users want to be able to quickly and easily use the authenticated credentials for:

- **Checking into or unlocking doors of home-sharing services**
- **A secondary form of authentication that supplements or replaces username and password**
- **Authorizing high-risk transactions such as wire transfers, online purchases or adding payees**
- **Age verification**
- **Password resets and other user credential updates**
- **Continuous security for authenticating ride-share drivers or delivery services**

Quick Incident Response

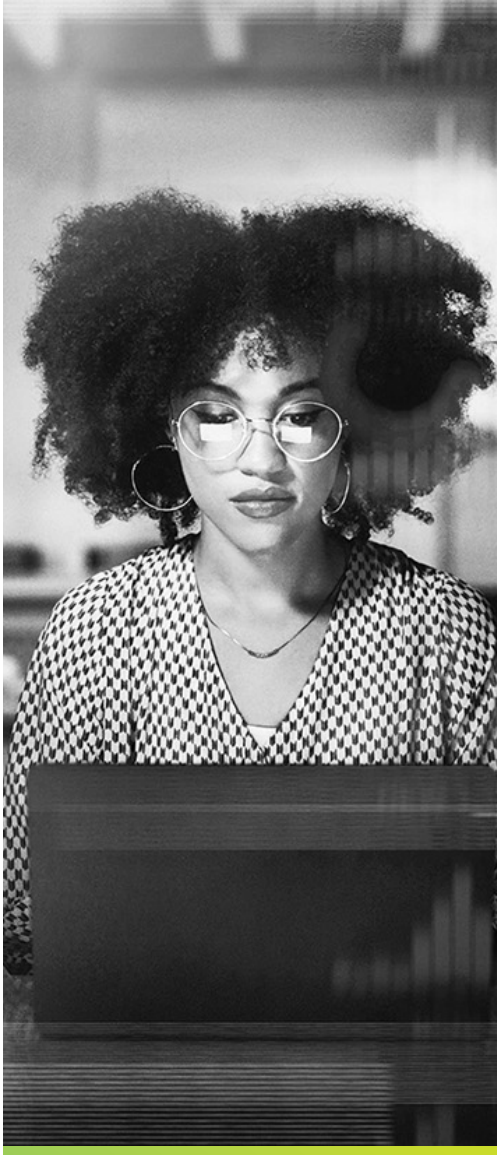
If a user has had a negative outcome, such as reporting the home they booked was dirty, they want easy access to customer support and/or a fast response to the incident.

Business Concerns

Sharing service companies have many of the same trust and safety concerns as their users, including:

- **The physical safety of their community members**
- **Account takeovers, bots and fake accounts**
- **Payment fraud and identity theft**

In addition, businesses face challenges that are unique to their supply-side part of the equation. Paradoxically, these issues are sometimes in direct conflict with the concerns of consumers.



Accuracy of the Identity Verification Experience

Customers want the experience to be fast and friction-free, while businesses want accurate identity verification — every time.

While striking that balance has been a challenge in the past, you can now create dynamic workflows that streamline the process. For example, you can run low-friction risk checks on the user's device and email, and then introduce more checks only if the risk is elevated — or right before they perform a high-risk action such as changing their password or transferring money. This allows you to onboard users much faster while protecting your platform.

Ongoing Monitoring

Once a participant has passed the initial vetting process, businesses must continue to monitor and/or periodically re-verify them to protect their brand. On the flip side, you don't want an obtrusive ongoing authentication process that risks alienating users or leads to attrition. Investing in an online identity verification system that verifies users' information and keeps their credentials updated as seamlessly as possible is key.

Regulatory Issues

The tremendous growth of the sharing economy has led to a reshuffling of regulations to accommodate this new economic model, while at the same time trying to maintain a level playing field for businesses using a more traditional marketplace model. Until regulations have caught up, sharing service providers are building their own self-governance systems.

Some home-sharing services, for instance, have faced pressure from local municipalities to release data on their providers. Airbnb chose to release anonymized data from five boroughs to New York in an effort to be transparent, while still protecting the privacy of its hosts. The data showed that most hosts were average citizens earning extra income, not landlords or hotel operators trying to game the system.

Companies in the sharing economy ecosystem are mobilizing to create their own set of self-governing principles to demonstrate they share a common purpose of operating responsibly, that they are open and transparent.

Content Abuse

Even with good policies in place, bad actors always find ways to game the system. One popular method has the provider setting up a seemingly legitimate account, but then communicating with users outside of the platform once initial contact has been made. Freelancer has banned unscrupulous employer providers like these from its platform after learning they were accepting bids from freelance users outside of the system. In some cases, this enabled the provider to avoid project fees, but in more severe cases, the provider would skip payments entirely, leaving the freelancer holding the bag.

The Battle for Market Share

"Sharing platforms will need to act fast in this competitive market. Both merchants and users are especially loyal in the sharing economy, often seeing themselves as part of a tight-knit community. Once they get set up, it's really hard to get them to move to a competing platform. As a result, there's a huge battle going on to onboard users as quickly as possible in these emerging markets. Stickiness will be important, and whoever is able to provide a unique and consistent experience for an exploding customer base will be primed to carve out market share."

Source: InformationWeek.com, Lessons We Can All Learn from the Sharing Economy

How the Industry Is Working to Instill Trust and Safety

Companies that use the sharing model all depend on one thing — trust. Charles H. Green, founder of Trusted Advisor Associates, describes a fundamental shift driven by the sharing economy from an infrastructure that relies on private ownership, insurance, lawyers, employee training and contracts to protect people from one another, to an infrastructure designed to *help people trust one another* through shared (or rented) ownership.

The trust equation in the sharing economy has three variables: the user (e.g., the one that wants to rent a home), the provider (e.g., the person who owns the home), and the brand community (e.g., the company providing the means by which the user and provider meet).

Successful Trust and Safety Business Model

USER Trust + **PROVIDER Trust** + **BRAND Trust**

Trust has to be established at every level of the transaction for it to be successful. What follows are some of the strategies the industry is using to instill trust and safety at every intersection of the sharing model.

Identity Verification

The oft-used term in peer-to-peer transactions is “trust, but verify.” Unfortunately, there is no one standard for online identity verification. While Americans, for instance, are familiar with offline IDs required for voting, flying or purchasing liquor, the concept of what constitutes a verifiable digital ID is still evolving. Nonetheless, identity verification is one of the chief tools for establishing a basis of trust at both the user and provider levels.

Verified IDs

In the same way that social media companies use verification symbols to indicate the “real, verified ID” for businesses and public interest accounts, sharing economy companies are beginning to adopt a similar concept to indicate a user has been verified to be who they claim to be. Freelancer.com, for example, gives both its project workers and project employers the opportunity to verify themselves through a combination of email, phone and social media profile verification. The aim is to provide both parties another level of assurance. The company even has a Freelancer Trust Score for those willing to put in more effort to instill trust.

Reviews and User Data

Nearly every sharing company relies on user and provider reviews. It’s not a surprise, considering multiple studies confirm that buying decisions are influenced by reviews. Podium found that 93 percent of consumers said reviews had an impact on their purchase decision. Consumers want to read about the experiences of others like them before entering a high-trust transaction.

Companies like UrbanSitter take things a step further by sharing data such as how quickly a sitter gets back to a family or how many times a sitter is asked back by the same family. By allowing providers and users to evaluate one another, the company adds one more rung on the trust ladder.

Organizational Trust Initiatives

Companies that offer shared workplaces are increasingly implementing Trust and Safety initiatives. They range from publishing defined principles around trust and support, like the one at TaskRabbit, to creating organizational workplace initiatives. Many organizations have established dedicated executives for Trust and Safety, including UpWork, Lime and Zeel.

NewCities, the non-profit group focused on shaping better urban futures, even launched a major research initiative to look at the impact of collaborative consumption on social trust in cities.

Redefining Regulations

As old business models fall away, creative new solutions are taking their place. Liability insurance has become a major regulatory issue in the sharing economy, given there are multiple parties — usually strangers — coming together to do business. There's the company that provides the platform (e.g., Lyft), the providers of the service (e.g., Lyft drivers) and the consumers of those services (e.g., riders). The primary issue for insurance regulators is who is liable if something bad happens: the individual providing the good or service, the user of the service, or the company who made the match?

In 2015, Uber and Lyft worked with the insurance industry to develop model legislation, called the Transportation Network Company (TNC) Insurance Compromise Model Bill, to bring clarity to TNC insurance laws across the country and eliminate consumer confusion. Historically, ride-sharing drivers were always required to have personal auto insurance policy, however the exclusions in those policies varied by person and by policy. The Insurance Compromise Model Bill sought to close those gaps by more clearly defining what coverage was mandatory and who would be responsible in the event of an incident. Many states have now adopted this bill.

Challenges with Online Identity Verification

Finding an online verification system that is accurate, fast and accessible is the primary barrier facing players in the sharing economy.

Online verification poses several huge challenges, including lack of consistent official IDs from country to country (or even state to state), difficulties matching a person to their official ID and technological disparities in authentication methods.

Additionally, verification solutions often need to be compliant with Know Your Customer (KYC), Anti-Money Laundering (AML), Bank Secrecy Act (BSA), General Data Protection Regulation (GDPR), Payment Services Directive (PSD2) and Payment Card Industry (PCI) regulations.

Identity verification includes three main steps:

1.

Verify the ID is authentic and valid

2.

Verify the person presenting the ID is the same person shown in the photo and is physically present during the transaction

3.

After onboarding, verify the person delivering or consuming the service is the same person who created the account

Historically, the verifications were done in person, usually at the place of business (e.g., the DMV, a bank). The user brought in various forms of identification, such as a birth certificate or Social Security card, and, because they were there in person, the agent could do a simultaneous visual identity check. It was more straightforward to root out certain types of fraud in these circumstances, but the verification process was inconvenient and took the user's valuable time.

Today, the opposite is true. It's more convenient for a user to verify their identity online, but the tradeoff is that it's also easier for users to create fraudulent identities by manipulating any of these steps.

Because detecting fraudulent IDs online is highly complex, there are many challenges to overcome, including:

Variety of ID Types

From national cards to passports to driver's licenses to biometric cards, there are an estimated 5,000+ types of identity documents that must be evaluated and authenticated for online verification.

Accuracy and Fraud Detection

Each one of these documents must be validated for authenticity. This includes checking for blurriness, expiration date and evidence of digital alterations.

Speed of Authentication

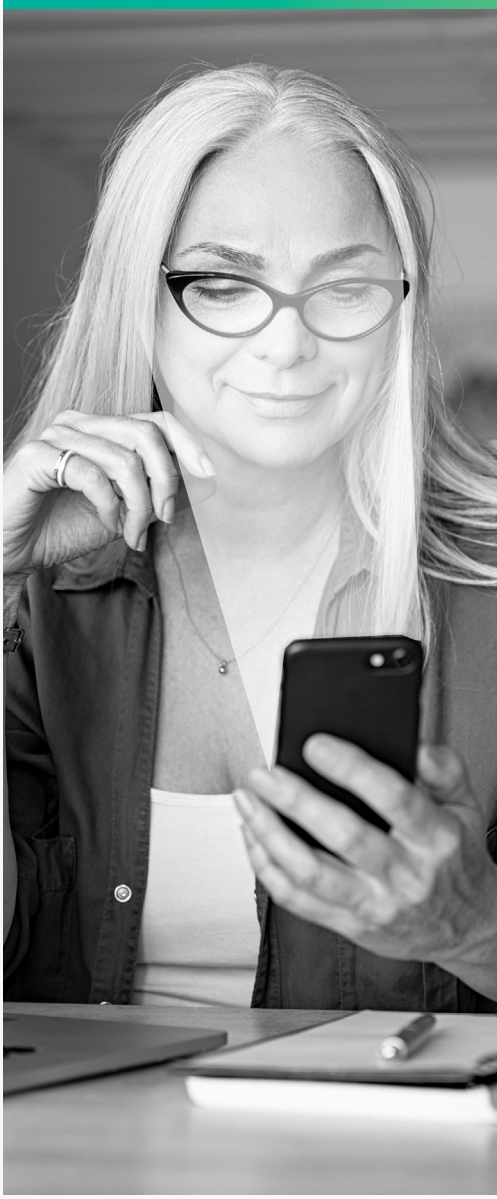
While they expect due diligence to be performed during the authentication process, consumers also expect to have near real-time verification, not to wait hours, days or weeks. Often, these two concepts are at odds with one another.

User Experience

Processes that make the gathering and capturing of ID documentation cumbersome lead to increased abandonment and lower online conversion rates.

Compliance

Beyond verifying documentation authenticity, providers must have data protection systems in place to store the consumer credentials in compliance with PCI, KYC and other regulations. This includes government-issued IDs, selfies and any biometrics captured during the verification process.



Five Elements of a Successful Solution

By now you understand that online identity verification is important to building trust and safety. So how do you know what to look for in a verification solution? Experts agree that solutions should aim to address these five important pillars.

1 Leverages Government-issued ID + Selfie

Because of massive data breaches and advanced hacking threats, companies should no longer rely on knowledge-based or SMS-based two-factor authentication. An authentic government issued ID, paired with a selfie, is still the most reliable and trusted form of identification.

To enhance the user experience, companies should let users choose between various forms of official IDs such as a driver's license, passport or ID card from a wide variety of countries and territories.

2 Employs State-of-the-Art AI and Machine Learning with Big Data

Today's sophisticated ID verification systems use artificial intelligence to quickly extract data from government-issued IDs and assess the likelihood of fraud or digital manipulation. But the machine learning models must be trained on vast, diverse data sets to ensure accuracy and minimize bias. Look for providers who process high volumes of transactions and are constantly evolving their technology.

3 Performs Liveness Detection for Onboarding and Authentication

Liveness detection ensures the person behind the transaction is physically present and not a spoof, such as a photo or video injection. This is important during onboarding, but it is even more important when a customer wants to perform a higher-risk activity such as changing their password or transferring funds over a certain amount. Be sure to choose liveness detection that is both sophisticated and easy to use.

4 Meets Compliance Mandates

Any system should help you comply with regulations and directives including AML, KYC, GDPR and PSD2 with a solution that spans international borders and ID types. In addition to stopping fraudsters, consider using an AML Screening solution to keep money launderers and sanctioned individuals off your platform.

5 Optimizes the User Experience

To maximize conversions, the verification process has to be quick, accurate and easy to complete. Minimizing the number of screens and clicks it takes to complete the application, pre-populating forms, providing clear instructions in plain language, enabling the user journey on mobile devices as well as laptop computers, and offering accessibility features (e.g., larger font size) are all ways you can enhance the user experience.

How Jumio Can Help

Jumio uses end-to-end AI-powered identity verification and authentication to foster trust and safety within some of the world's top sharing economy brands. We leverage an innovative mix of machine learning and AI, biometric technologies and the world's leading data scientists to determine if government-issued IDs are authentic and belong to the user. We protect our customers' ecosystems against reputational threats and physical risk across a wide range of scenarios.

We've processed over one billion transactions and protected companies around the world, and we'd love to help yours as well. **Contact us** to learn more about keeping your ecosystem trusted and safe.

More Platforms

iOS, Android and webcams

More Accurate

99.95% valid customers approved and 95% invalid customers rejected (based on audited results)

More Technology

Biometrics, computer vision, augmented intelligence, machine learning and verification experts

More Security

PCI, KYC, AML, PSD2 and GDPR compliance coupled with strong encryption

More Countries

Supports ID documents in more than 200 countries and territories

More ID Types

Supports thousands of passports, driver's licenses and ID cards, including older versions