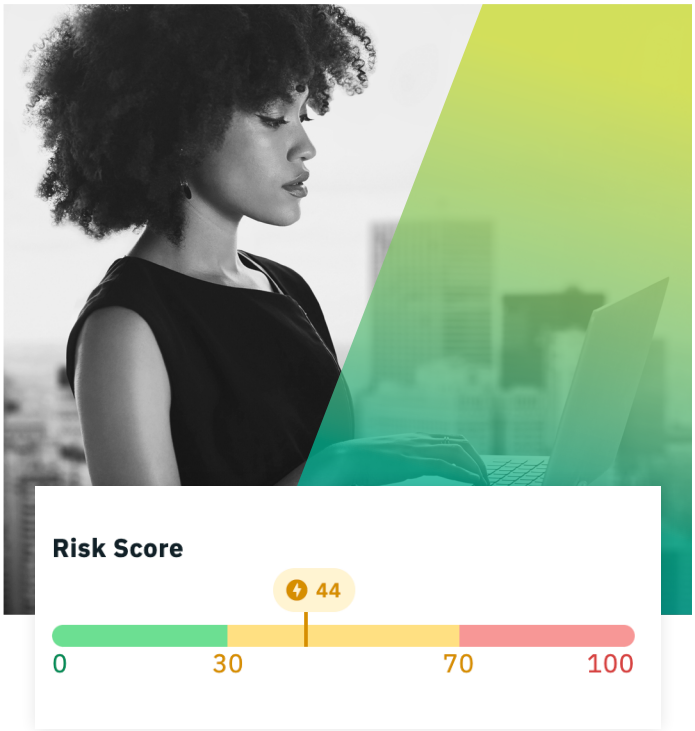
jumio | Risk Signals

Mitigating Risk Throughout the Entire Customer Lifecycle

For many businesses, identity proofing requires more than just checking an ID. Jumio's advanced risk signals provide additional assurance and trust that your customers are who they say they are — and that they do not provide unnecessary risk to your business — during onboarding and each time they return to your platform.

Jumio's comprehensive data hub provides access to 500+ data sources to confirm your customers' personally identifiable information (PII) and assess their risk. A composite risk score makes it simple to get a yes/no answer and to automatically drive decisions in your workflows.

Following are some of the key risk services Jumio provides.



Global Identity Check

Run the user's name, address, phone and email through a network of global identity databases to gain assurance that they belong to this person and to assess the person's overall risk. This service determines the validity of each data point — such as verifying that the email actually belongs to this person — and determines risk based on behavior, such as assigning higher risk if the phone is associated with many IP addresses. After evaluating all of these factors, the service returns a single risk rating for the person, which you can then use in your rules to trigger more stringent KYC procedures as needed.

This service is especially useful as a lightweight check at onboarding to determine whether further checks are needed, or for ongoing risk monitoring of your existing customers.

Government Database Checks

Verify that the data provided by the user or extracted from the ID card matches the data held by the jurisdiction that issued the legal document.

This service checks government databases around the world.

Social Security Number Check

Verify that the name and address (and optionally the date of birth and phone number) match the Social Security number by checking databases from the Social Security Administration, USPS, credit bureaus and other proprietary sources.

This service is useful as a lightweight check for U.S. users.

Phone Number Check

Determine the risk and reputation of a phone number. This service looks at usage patterns (including voice traffic), usage velocity and phone data attributes like phone type and carrier information. It also checks the number against the Global Phone Data Consortium for fraud history, evaluates messaging behavior and identifies whether it's within a range of phone numbers that are seen repeatedly on one or more web services, which could indicate that a digital profile is being shared.

The service returns a risk rating and additional data that can guide your workflow, such as requiring users with blocked phone numbers to enter an unblocked number.

Email Check

Assess the risk of an email address by evaluating its velocity, age, domain details, country, fraud history and other details.

This service returns detailed information about the email address so you can make an informed decision.

Address Checks

Validate and corroborate addresses with independent, third-party sources. Determine whether the address extracted from a government-issued ID exists in the real world, and see if the person being verified actually lives at the address on their ID. Jumio checks the address against a number of trusted data sources (e.g., USPS, Royal Mail) to properly format the address, ensure it exists in a given jurisdiction, and verify that the person lives there.

This service is useful for complying with regional regulations that require you to validate addresses and establish proof of residency using independent public sources.

Device Check

Assess the risk of the user's device through indicators such as extensive device history, fingerprinting anomalies, usage patterns and emulators. Find out if a fraudster is using GPS emulation, device rooting or proxies to mask its high-risk location and trick your online identification flow.

Because this service runs in the background before the user has entered any information, it's an excellent, frictionless check to run at the very beginning of the onboarding journey or digital transaction.

Geo IP Check

Check the risk and reputation of the user's IP address and determine their ISP's location.

This service is especially useful for stopping the user journey before it starts if the user is attempting to hide their actual location or if their IP address has unusually high velocity that can be attributed to a bot.

BIN Check

If you request a payment card from users during onboarding, use the bank identification number (BIN) on that card to get information such as the bank name and country and the card type.

This service is useful for flagging prepaid cards, cards that were issued in a different country from the user's residence, and corporate cards (which are not acceptable for online gambling).

Which Risk Signals Do I Need?

All businesses can benefit from checking the device reputation before the user even enters their name, allowing you to divert suspicious users to more rigorous workflows while streamlining the experience for your good customers. You can also run the global identity check to filter out suspicious identities before performing more stringent checks. You can check the user's IP address to prevent users in prohibited locations from accessing your platform. Similarly, if you enable customers to transfer money to each other, you could determine whether the transaction is taking place in a high-risk location that would necessitate more stringent KYC or AML checks. And for even greater scrutiny, you could perform address, phone and email verification and government database checks during onboarding and run global identity checks periodically on existing customers. Jumio makes it easy to choose the risk signals that meet your specific business needs and risk tolerance.