PLAID

Plaid IDV's Risk & Fraud Checks

A deeper dive into Plaid's fraud engine

99%

Accuracy in determining return users with Plaid's risk & fraud signals

1000's

Of data points analyzed instantly to protect you from fraud

Identity Verification uses many powerful tools to help detect fraud and protect your platform from bad actors. Below is a brief overview of various checks that are done whenever a user moves through Identity Verification. Though not absolutely comprehensive, it covers our general approach to detecting fraudulent activity. As you review these different checks, please remember that no single check gives a conclusive yes or no as to whether the user is fraudulent. All of the checks we perform need to be considered holistically

Fingerprinting

When the end user opens the Identity Verification UI , we start by "fingerprinting" the session by looking at hundreds of different attributes, including:

- IP Address
- Location
- Browser plugins used
- Browser and OS settings
- WebGL parameters
- User agent details
- TCP settings
- Cookies
- Screen resolution
- Battery usage
- Device memory

PLAID

Device & IP Address Checks

On top of using IP Address for fingerprinting, we do a number of IP fraud checks:

- Proxy, VPN, and Tor detection - We detect whether the user is using a VPN or Tor. Using a VPN is correlated with a slight increase in fraud risk, using Tor is associated with a very high fraud risk. We also check if a public or web proxy is being used.
- Abuse lists - We check a number of IP abuse reporting lists to see if the user's IP is associated with a large number of spam complaints. This can often be an indicator that the user's machine is compromised by malware and increases potential risk of fraud.
- Data Centers - We detect if the user's IP is associated with a datacenter, which is correlated with abuse.
- IP geolocation country mismatch - We report if the user's IP address is associated with a different country than they provided as part of the KYC data they provided.
- IP geolocation device timezone mismatch - We report if the user's IP address is associated with a country that is in a different timezone than the one we detect as part of the device fingerprinting.
- Open ports - We check for any suspicious open ports, as well as whether port 80 is open on the IP Address.
- Incognito session - We detect whether the user is going through the Identity Verification session in a browser that's in incognito mode.

Email Checks

We support (and highly recommend) providing a user's email address when doing a verification so it is associated with the session. If it is provided, we perform these checks:

- Disposable emails - We check to see if the user is using one of many hundreds of different disposable email services (for example, Mailinator). This signal is highly correlated with fraud.
- Email deliverability - We do a live check on the domain associated with their email to see if it is actually configured to receive email. Failing this test means the email is fake which is a strong fraud signal.
- Recent domain registration checks - For emails using custom domains (for example, “@plaid.com" would be a custom domain and "@gmail.com" would not), we check when that domain was registered. Emails associated with domains registered in the last 3 months are correlated with fraud risk.
- External account registration checks - We do a live check against ~90 different popular social networks and services to see if this email is registered on other services. If it's linked with many different services, that is a strong positive signal. Conversely, failing to link to any services is viewed as a risk. If no services or very few services link to the given email, we show a medium or high risk flag in the risk section of the dashboard. Otherwise, we show icons in the sidebar for all accounts linked.
- Email data breach checks - We check services like Have I Been Pwned to see if the user's email has shown up in known breaches. Specifically, we record 1) How many different data breaches has this email shown up in? And 2) How long ago was the first data breach, and how recent was the most recent breach? This check is very neat and a bit counter-intuitive: it is a strong positive signal if the user's email has been found in many data breaches, and it is especially positive if, for example, the dates of those breaches go back 5+ years. We treat this as a positive signal because it indicates that the email is authentic and actively used. As a proxy for the age of an email address, this is a powerful check to catch disposable traits that use reputable services. Likewise, an email not being found in any data breaches is correlated with fraud risk for a similar reason as

not being linked to external services. It suggests the email is disposable.

Phone Checks

We perform an external account registration check on the user's phone number as well. We check 14 different services to see if the user's phone is linked to accounts elsewhere on the web.

Stolen Identity & Synthetic Risk Scoring

By analyzing data such as name, email, phone number, email, address, birthday and social security number, we can provide a score from 0-100% indicating the likelihood the provided identity has been stolen, falsified, or fabricated. Our models have been trained on millions of identities and third party data such as credit header files, phone carrier records, bankruptcies and many more to accurately assess and predict the likelihood of identity theft or manipulated identities.

For example, stolen and synthetic risk scoring conducts checks such as:

- If the PII is associated with a deceased individual
- How many identities are associated with a phone number or email
- If a user has history associated with another social security number
- Whether the social security number issuance aligns with the user’s history
- Length of time a user leverages the provided social security number
- Length of history of phone and email addresses

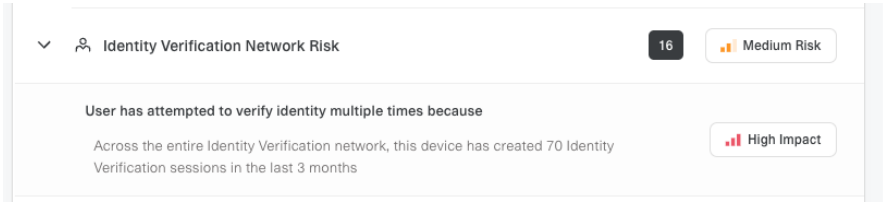
Network Risk

As mentioned in the fingerprinting section, we perform a highly accurate check that helps us detect if we have seen the current user before. This check is consistent and reliable even over months of time as long as the user visits from the same computer. We track how many times we've seen a specific device create separate Identity Verification sessions, both within your integration and

across our platform, and we estimate risk from that based on the time frame within which those separate sessions were created. We view it as risky if multiple sessions are created on your platform in the same day or week, since this is likely a user with multiple accounts on your service. Likewise, we look at account velocity during the last 3 months across our entire network in order to flag devices that seem to be creating a large amount of accounts across different services.

We check for:

- Number of Identity Verification session across the entire network in the last 3 months
- Number of Identity Verification sessions for your organization in the last 24 hours
- Number of Identity Verification sessions for your organization in the last 7 days
- Number of Identity Verification sessions for your organization ever



Behavioral Analytics

When the user goes through the Identity Verification UI (note this cannot be done if using Database verification via API only), we monitor and assess how a user enters their PII to assess how familiar they are with it or if they exhibit behavior that's typical of fraud rings or bots. We look at things like:

- How fast a user types in their PII
- How accurately a user enters their PII
- Method of data entry and whether the data is copied and pasted
- The order in which a user inputs data

If the exhibited behavior is consistent with bad actors, fraud rings, or bots, we flag these behaviors and provide a "User Behavior" risk level. Based on the acceptable risk level set, Identity Verification

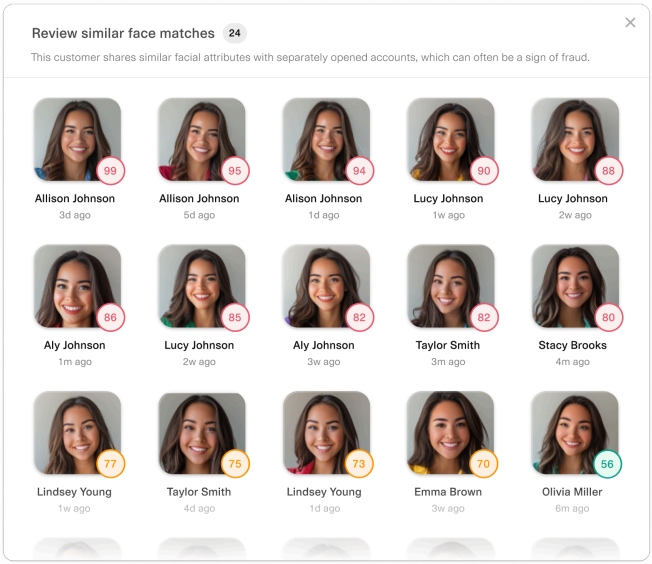
will either prevent a risky user from completing the signup process or simply inform you of the risk level.

Facial Duplicate Detection

Plaid Identity Verification can now automatically flag duplicate users and potential fraud by matching user selfies against your entire user base. This provides you with significant protection against account takeovers and incentive abuse, without any changes to your UX. Facial Duplicate Detection features include:

- Prevent fraudsters from tampering with IDs and signing up multiple times by cataloging their faces
- Duplicate matching across both selfies, and document portraits
- Incredible accuracy with a 1:1M false match rate
- Match across your entire user base or just within specific use cases – flexible for your specific needs

To start using Facial Duplicate Detection today simply turn the feature on within your Plaid Identity Verification editor - zero changes to your integration are needed.



PLAID

plaid.com

Plaid is a global data network that powers the tools millions of people rely on to live a healthier financial life. Our ambition is to facilitate a more inclusive, competitive, and mutually beneficial financial system by simplifying payments, revolutionizing lending, and leading the fight against fraud. Plaid works with over 8,000 companies including fintechs like Venmo and SoFi, several of the Fortune 500, and many of the largest banks to empower people with more choice and control over how they manage their money. Headquartered in San Francisco, Plaid's network spans over 12,000 institutions across the US, Canada, UK and Europe.

Questions? Reach out to our sales team at info@plaid.com.