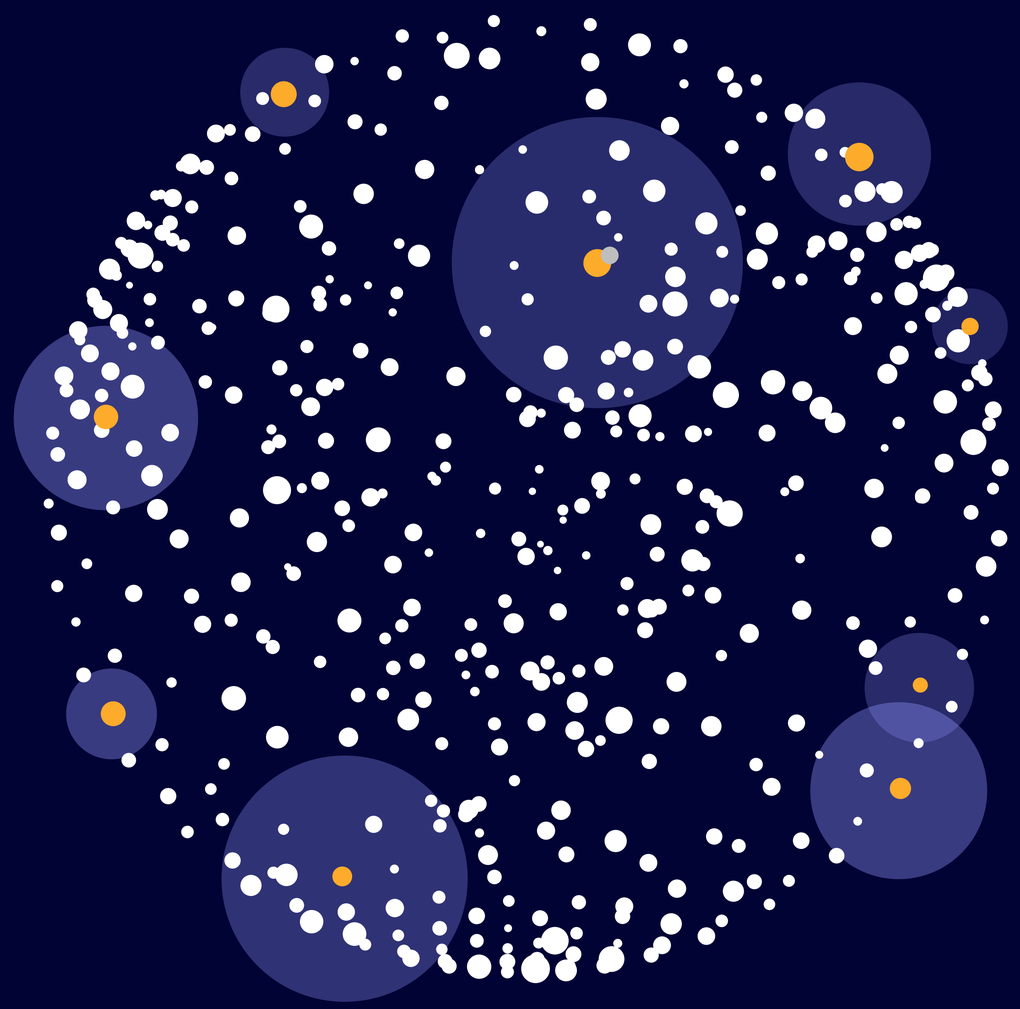
persona

50+ risk signals of fraud

Learn how signals are used to create a more nuanced understanding of a user's risk profile so you can make better-informed decisions in real time.



As you likely know, fraud today comes in many forms.

In our work with hundreds of companies, we've found that the most effective ones take a holistic approach to fighting fraud: they examine multiple user signals, they combine data points, they analyze population-level trends, and they actively segment users based on risk level.

In this asset we lay out 50+ signals we recommend teams look at to assess the risk level of any user, or group of users. Note that this is not a comprehensive list! It's just meant to be a resource as you assess your own strategy, and an insight into signals you may want to add.

Find out how our risk signals strengthen your fraud strategy.

Glossary of terms

Types of signals	Types of fraud
Active signals Signals that depend on the user taking an action before you can run a fraud or identity check (if you would generally run that fraud or identity check as a standalone check). These could include signals based on checking the user's email, phone number, ID document, selfie, etc.	**First-party fraud** This happens when a person intentionally misrepresents themselves to deceive a business or other institution. It most commonly involves a fraudster submitting false information.
Passive signals Signals based on information the user didn't actively submit, such as an IP address or device fingerprint. Passive signals also include signals from checks you generally wouldn't run as a standalone fraud or identity check, such as a SIM swap check.	**Second-party fraud** This happens when one person willingly gives their information to someone else, and the second person uses that information to commit fraud.
Behavioral signals Signals based on activities a user takes while on your platform. This can include time it takes a user to complete a given activity, number of times a user autofills a field, number of times a user employs a keyboard shortcut, etc.	**Third-party fraud** This happens when a person's identity or details are used without their consent or knowledge. Often the result of a hacking attack, data breach, or phishing attack.

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	Fraud use case(s)	Type of fraud	Learn more
1	☐	**IP address**	An IP address can give information around risk, such as significant differences between the location of the IP address at the time of verification and the address on an ID or an attempt by the user to obfuscate their IP address via a VPN.	Passive	All	Third-party	Fraud detection: 5 methods to protect your customers and business
2	☐	**Proxy and Tor**	The use of proxies or tors can indicate that a bad actor is trying to obfuscate their identity by concealing their point of origin or internet connection.	Passive	All	Third-party	Fraud detection: 5 methods to protect your customers and business
3	☐	**Geolocation**	Risky geolocations can be indicate bad actors looking to obfuscate their identity or circumvent deny lists.	Passive	All	Third-party	Fraud detection: 5 methods to protect your customers and business
4	☐	**Internet service provider (ISP)**	Little-to-unknown ISPs (e.g., non-commercial or residential providers) can be a signal of an individual looking to obfuscate their digital footprint.	Passive	All	Third-party	Fraud detection: 5 methods to protect your customers and business
5	☐	**Device fingerprint**	Device fingerprinting is the process of collecting information about a device, such as a device's hardware and software, to identify and prevent fraud.	Passive	All	Third-party	How device fingerprinting catches suspicious actors
6	☐	**Browser fingerprint**	A browser fingerprint is a unique string that documents a specific interaction between a web browser and a device.	Passive	All	Third-party	Using browser fingerprinting to deter repeat fraud
7	☐	**Phone risk score or report**	A phone number allows you assess a user's validity and reputation by analyzing carrier signals, velocity, VOIP detection, and 3rd party consortiums.	Passive	All	First- and third-party	Assess phone numbers and emails for risk
8	☐	**SIM swap**	SIM swap fraud occurs when a scammer transfers a phone number to a new SIM without the owner's authorization. Scammers can then intercept texts, including one-time passwords (OTPs), and try to break into a victim's accounts.	Passive	All	Third-party	Phone verification: An important part of identity verification and fraud prevention
9	☐	**Carrier PII match**	Phone numbers are cross-referenced against consumer and telecommunications data that binds a number with a physical identity.	Passive	All	Third-party	Phone verification: An important part of identity verification and fraud prevention
10	☐	**Email risk score or report**	An email address allows you assess a user's validity and reputation through signals such as email age, velocity, and 3rd party consortiums.	Passive	All	First- and third-party	Assess phone numbers and emails for risk

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	Fraud use case(s)	Type of fraud	Learn more
11	☐	**Email identity binding**	Emails are cross-referenced against consumer data sources that bind emails with a physical identity.	Passive	All	Third-party	How email verification can help you confirm identities and prevent fraud
12	☐	**Matching data with a known bad actor(s)**	Link analysis prevents fraud by identifying accounts connected by suspicious shared details.	Passive	All	Second- and third-party	Link analysis: How can it help you spot fraud?
13	☐	**Selfie repeat**	When a user's selfie submission matches a selfie from another account, it can indicate fake identities or other fraud.	Passive	All	Second- and third-party	The strategic guide to fighting GenAI fraud
14	☐	**Background repeat**	When a user's photo background submission matches the photo background in another account, it can indicate fake identities or other fraud.	Passive	All	Second- and third-party	The strategic guide to fighting GenAI fraud
15	☐	**Watchlist screening**	A watchlist report screens an individual's information across 100+ global sanctions and warning lists.	Passive	Money Laundering	All	Meet global AML compliance with watchlist screenings
16	☐	**Politically exposed person (PEP)**	A PEP report screens an individual to determine if they are an individual who is or has been entrusted with a prominent function by a governmental body.	Passive	Money Laundering	All	What is a politically exposed person (PEP)?
17	☐	**Social media lookup**	A social media report enriches an individual's profile with details about their social media accounts.	Passive	Money Laundering	All	Use social media signals to better assess risk
18	☐	**Adverse media check**	An adverse media or "negative news" report is any unfavorable information found across a wide variety of news sources, including traditional news outlets and unstructured sources.	Passive	Money Laundering	All	Mitigate risk via automated adverse media screening
19	☐	**Address lookup**	Evaluates information about an address, like delivery point (address exists and can be delivered to), address type (residential or commercial), and congressional district.	Passive	All	All	What is address verification?
20	☐	**Bank verification**	Verifies bank accounts during onboarding, often to comply with marketplace regulations.	Passive	Misrepresentation of personal data	All	Explore our marketplace of 3rd-party partners

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	Fraud use case(s)	Type of fraud	Learn more
21	☐	ID theft score	Helps ensure that each identity isn't a stolen identity.	Passive	Identity Theft	Third-party	Explore our marketplace of 3rd-party partners
22	☐	Synthetic risk score	Helps ensure that each identity (name, date of birth, and SSN) corresponds to a real person, and isn't a synthetic identity.	Passive	Synthetic Identities	First- and third-party	Explore our marketplace of 3rd-party partners
23	☐	Completion time	Time duration from start to finish of flow	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
24	☐	Distraction events	Number of times the user left the flow	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
25	☐	Hesitation percentage	Percentage of time in the flow where the user made no inputs.	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
26	☐	Shortcut usage (copies)	Number of times user used a keyboard shortcut to copy information.	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
27	☐	Shortcut usage (pastes)	Number of times user used a keyboard shortcut to paste information.	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
28	☐	Autofill starts	Number of times the user autofilled a form field.	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
29	☐	Number of verification attempts	Evaluate how many times it takes a user to verify their identity.	Behavioral	All	Third-party	Learn more about Persona's behavioral signals
30	☐	Phone 2FA	Uses two-factor authentication to confirm that users owns the phone numbers they submit.	Active	All	Third-party	Phone verification: An important part of identity verification and fraud prevention
31	☐	Email 2FA	Uses two-factor authentication to confirm that users own the email addresses they submit.	Active	All	Third-party	How email verification can help you confirm identities and prevent fraud

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	Fraud use case(s)	Type of fraud	Learn more
32	☐	**Email authentication**	Establishes ownership of an email account and authenticates that the address is reputable.	Active	All	First- and third-party	How email verification can help you confirm identities and prevent fraud
33	☐	**Valid tax ID number (e.g., Social Security number)**	Verifies that the Taxpayer Identification Number (TIN) is valid and current.	Active	All	Third-party	The strategic guide to identity verification
34	☐	**Failed name and tax ID comparison**	If the database check between name and TIN does not register a match, you can ask for additional information to validate the combination of PII submitted.	Active	All	All	The strategic guide to identity verification
35	☐	**Address on the submitted ID is to a PO Box**	This might require additional follow-up information to validate that the PO box provided is connected to the user verifying their identity.	Active	All	All	The strategic guide to identity verification
36	☐	**Tampered ID image**	If a submitted image is tampered by a photo editor, you can ask the user to resubmit the image and limit the number of verification attempts.	Active	All	Second- and third-party	The strategic guide to identity verification
37	☐	**Barcode is not legitimate**	Capture and analyze the barcode to ensure that information submitted is legitimate.	Active	All	All	The strategic guide to identity verification
38	☐	**Data extraction inconsistencies**	Relevant ID properties (e.g. name, birthdate) extracted from the front of the ID are different from the details extracted from the barcode.	Active	All	All	The strategic guide to identity verification
39	☐	**Confirm through active and passive selfie liveness the genuine presence of an individual**	Liveness detection is an important tool to assess the genuine presence of an individual. Active selfie liveness techniques require the individual to take an action, such as a hand wave or smile. Passive liveness techniques look at things like micromovements in the face, 3D depth analysis, and light reflections.	Active	All	Second- and third-party	What is liveness detection?
40	☐	**Failed selfie-to-ID comparison**	When a selfie taken in real time does not match ID portrait, it can indicate fraud.	Active	All	All	What is liveness detection?
41	☐	**Failed 3-point composite check**	You can verify users in real time and catch common spoofs with 3-point checks. If a user fails a 3-point check because of a failed pose, you can require a user to retry their submission.	Active	All	All	Seamless selfie liveness verification

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	Fraud use case(s)	Type of fraud	Learn more
42	☐	**An electronic replica is detected**	Checks that a document isn't an electronic replica (digital text, digital icon, screenshot, etc.). When electronic replicas are submitted as documentation, it can indicate that documentation may be altered.	Active	All	Second- and third-party	What is liveness detection?
43	☐	**Discoloration of the ID submitted**	The colors on an ID are different than the colors you'd expect.	Active	All	Second- and third-party	What is liveness detection?
44	☐	**Glare and blur detection**	Detects if a submitted ID has glare or blur that would make it difficult to verify an identity.	Active	All	All	What is liveness detection?
45	☐	**Age estimation is below required threshold**	The estimated age is below the age required for a delivery purchase such as alcohol or tobacco.	Active	All	First-party	How to add the right age verification system to your business
46	☐	**Virtual camera has been detected**	If a virtual camera is detected, there is a higher likelihood that the user is attempting to submit a fake image to pass liveness checks.	Active	All	Third-party	The strategic guide to fighting GenAI fraud
47	☐	**Poor video quality**	There a number of non-fraudulent reasons why video quality may be poor: a user's device, corrupt photos/ videos, low frame rate, short duration. Capturing quality video makes verification significantly easier.	Active	All	Second- and third-party	The strategic guide to fighting GenAI fraud
48	☐	**Photo submitted detected to be a print out**	An ID or selfie is printed on a piece of paper and held up to the screen.	Active	All	Second- and third-party	The strategic guide to fighting GenAI fraud
49	☐	**No match with a eCBSV database check**	Gains higher assurance of a user's identity by verifying their provided name, date of birth, and social security. If there is no match for the combination of personal identifiable information, there is a higher risk of an authentic fraud.	Active	All	All	What are issuing database verifications?
50	☐	**Failed document verification**	A document — such as a bank statement, employment record, business document, etc. — is determined to be not authentic.	Active	All	All	Document verification: Understanding the whole process

Risk signals from know your business (KYB) checks

The signals above can be important when you verify the identity of a business's ultimate beneficial owners or representatives. Additionally, the risk signals below may be specific to checks you run while verifying a business entity, such as a partnership, limited liability company, or corporation.

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal Signals related to the entity, not user interactions, will be passive or active.	The signal can help you answer: KYB risk signals help confirm a business's existence, gauge its risk, and determine if someone is an authorized representative.	Learn more
51	☐	501(c)(3) status	Checking a nonprofit's tax-exempt status with the IRS and in state registries can help you assess its legitimacy.	Passive	Does the business actually exist?	Charity verification for California AB 488 compliance
52	☐	Appearance in credit card panel data	A business's appearance in aggregated and anonymized credit card transaction data can lend credence to its legitimacy.	Passive	Does the business actually exist?	24 KYB risk factors you should consider
53	☐	Better Business Bureau (BBB) rating	A BBB rating can help you decide whether you want to do business with a company.	Passive	Is working with the business risky?	24 KYB risk factors you should consider
54	☐	Business address type	The business address type (commercial or residential) should match the business type and size.	Passive	Does the business actually exist? Is working with the business risky?	Make better decisions by assessing address risk.
55	☐	Business adverse media check	Adverse media may mean that a business you are considering working with is risky. A company that has engaged in financial crimes in the past, for example, may bear money-laundering risk for your business.	Passive	Is working with the business risky?	Mitigate risk via automated adverse media screening
56	☐	Business entity type	The entity type, such as sole proprietorship or partnership, can help you understand the business's ownership structure.	Passive	Does the business actually exist? Is working with the business risky?	KYB requirements for sole proprietorships vs. LLCs
57	☐	Business liens	Liens may indicate that a business failed to honor its obligations or may have difficulty meeting future obligations.	Passive	Is working with the business risky?	Glossary: Business lien

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	The signal can help you answer:	Learn more
58	☐	**Business watchlist screening**	Some organizations are on sanctions and watchlists, which may indicate the business is involved in money laundering or other illegal activity.	Passive	Is working with the business risky?	Meet global AML compliance with watchlist screenings
59	☐	**Business website verification**	A business's website provides additional context for assessing risk, including the domain's validity, name, and age. The presence of certain pages, such as about or terms of service pages, can also be relevant.	Passive	Does the business actually exist? Is working with the business risky?	24 KYB risk factors you should consider
60	☐	**Email risk score or report**	The age of an email address, a domain that matches the business's website, and the email's reputation score can help you decide whether you want to be associated with the business.	Passive	Does the business actually exist? Is working with the business risky? Is this person authorized to act on behalf of the business?	Assess phone numbers and emails for risk
61	☐	**Industry classification**	It can be risky to do business with companies operating in certain industries.	Passive	Is working with the business risky?	24 KYB risk factors you should consider
62	☐	**Listed on a stock exchange**	Public companies have strict reporting requirements, and knowing that a company is publicly listed can serve as a helpful measure of its legitimacy.	Passive	Does the business actually exist?	24 KYB risk factors you should consider
63	☐	**Recent formation date**	A recently registered or incorporated business may be riskier than an established one.	Passive	Is working with the business risky?	How to fight business fraud like a pro
64	☐	**Recent reactivation date**	A recently reactived business might be risky.	Passive	Is working with the business risky? Is this person authorized to act on behalf of the business?	How to fight business fraud like a pro
65	☐	**Social media presence**	Lack of social media activity or a new profile could be signs of risk, especially for consumer-facing businesses.	Passive	Does the business actually exist? Is working with the business risky?	Evaluate social media signals to better assess risk
66	☐	**Suspicious links to other businesses**	Multiple businesses and entities with shared attributes could be an indication of a fraud ring.	Passive	Does the business actually exist? Is working with the business risky?	Detecting fraud rings and protecting your business

	Are you tracking this currently?	Risk signal	Why it matters	Type of signal	The signal can help you answer:	Learn more
67	☐	**Bad or no credit history**	Businesses can have credit reports, similar to individuals, and a lack of credit history or bad credit might be a sign of risk. You can also compare information from the report to what you collect elsewhere.	Active	Does the business actually exist? Is working with the business risky?	What are issuing database verifications?
68	☐	**Business bank verified**	If someone can verify the business's bank account, that's a good sign that they are authorized to represent the business.	Active	Is this person authorized to act on behalf of the business?	How to build a Know Your Business (KYB) process
69	☐	**Inactive registration status**	Legitimate companies should register with the Secretary of State in every state where they do business. An inactive status may indicate the business doesn't exist or didn't register.	Active	Does the business actually exist?	KYB vs. KYC: What's the difference?
70	☐	**Inconsistencies between business documents and official filings**	The information from the business's internal documents should align with its public filings.	Active	Does the business actually exist? Is working with the business risky? Is this person authorized to act on behalf of the business?	Business impersonation: is your KYB strategy up to the challenge?
71	☐	**Invalid business registration number**	Some countries have official registries for businesses. The lack of a valid business registration number may indicate that a business is illegitimate or improperly registered.	Active	Does the business actually exist?	How to build a Know Your Business (KYB) process
72	☐	**Invalid TIN**	An invalid Taxpayer Identification Number (TIN), commonly an Employer Identification Number (EIN), may indicate the business isn't registered with the IRS.	Active	Does the business actually exist?	How to check if a company is legitimate: a step-by-step guide
73	☐	**Invalid VAT number**	Businesses operating in countries with a value-added tax (VAT) should have a valid VAT number.	Active	Does the business actually exist?	International KYB: Everything global businesses need to know
74	☐	**Lack of registration documents**	The lack of business registration documents, such as articles of organization/incorporation, may indicate that the business doesn't exist or a person doesn't have access to the documents.	Active	Does the business actually exist? Is this person authorized to act on behalf of the business?	Business document verification: What it is, why it's important, and how it fits into your broader KYB strategy