



SHORT GUIDE · RISK · IDENTITY FRAUD

New customer, fake identity?

Signals checked before you commit.

Anyone who signs up or applies for a contract starts by claiming who they are. This short guide shows how PaperOffice delivers email address, IP address, device and ID document as signals you can check. For shops, platforms, landlords and retailers selling on installments.

KEY TAKEAWAY

Every check returns fields your rule can act on: a recommendation for the email, flags for VPN and Tor, a device ID and ID document fields with their source location. Your team makes the decision.

01 · THE PROBLEM

The name is right. The person behind it is not.

A new customer signs a contract online, and the smartphone ships on installments. Name, address and email address look genuine. Only when the payments stop does it become clear: the data belongs to someone else, or the person does not exist at all.

WHY IT HAPPENS

Stolen and invented data

Fraudsters use real names and addresses from data leaks or mix them with invented details. On the form, both look the same.

Hiding on the network

Disposable addresses, VPNs, Tor and rented servers conceal who is ordering. The same person can open many accounts with little effort.

IDs in a hurry

At the counter, the ID copy gets a quick look and is typed in. A typo or a missing field easily slips through.

HOW YOU NOTICE IT

- The email address comes from a disposable service, or its domain has no mail server.
- The sign-up comes through a VPN, Tor or a data center instead of a regular connection.
- The country of the IP address does not match the stated address.
- The same device shows up in several sign-ups under different names.
- Details on the form and on the ID document differ.

02 · THE WAY WITH PAPEROFFICE

From signal to decision.

PaperOffice delivers signals on email, network, device and document, via REST API, SDK and in the app. What follows is up to your rule: let through, ask again, send to review or reject.

1

Assess the email address

POST /fakeemail/check checks disposable domains, MX records, SPF and DMARC and returns risk_score plus the recommendation ACCEPT, REVIEW or REJECT.

MODULE: [FAKE EMAIL DETECTION](#)

2

Check network and location

/ip2location/full returns country, region and provider, plus is_vpn, is_proxy, is_tor and is_datacenter. The type field names the list that matched.

MODULE: [VPN DETECTION](#)

3

Recognize the device

The browser SDK returns a visitor_id per device. At the next login, /fingerprint/verify checks whether it is the same device, and risk.factors names anything unusual.

MODULE: [DEVICE FINGERPRINT](#)

4

Read the ID document

An IDP Agent reads name, date of birth, address, document number and expiry date from a photo or scan, each value with its location in the original.

MODULE: [IDP AGENT](#)

5

Decide

Your application combines the fields into a rule, for example: a disposable address or Tor means review by a person. Your team makes the decision.

03 · IN THE APP

Keys, SDK, agent: how to set it up.

The signal checks run via REST API and SDK, the ID document via an IDP Agent in the app. The names match the app.

1

An API key for your backend

Under **API & Developer > API Keys**, use **Create New Key** to create an **API Key**. Your backend uses it to check email and IP. You can copy the key there at any time.

2

A key for the browser SDK

Under **API & Developer > API Keys**, use **Create New Key**, choose the type **Publishable Key** and enter your website's domains. Your site then loads the fingerprint SDK with it.

3

Create an IDP Agent for IDs

Select a sample photo, then **Actions > Agents & workflows > IDP** and **Create new agent**. Choose a template for ID documents or describe the fields in your own words.

4

Check values against the source

In the **Data Fields** tab, every value sits next to the snippet from the ID document. The **IDP Review** view shows all documents with open fields.

5

Work through review tasks

If a required field is missing, a task is created in the chosen review queue. Under **Workflow AI > Human In The Loop Tasks**, a person sees the ID and the fields and completes the review.

TIP FROM PRACTICE

Weigh several signals together A VPN on its own often has harmless reasons. It becomes meaningful together with a disposable address or a device that is already linked to other accounts in your system. Define when a person reviews.

04 · AN EXAMPLE

A phone retailer. Contracts with installments.



A mobile phone retailer with six stores and an online shop sells smartphones with contracts and installment plans. In the store, the team copies the ID and types in the data, online a form is enough. Time and again, payments stop and the customers cannot be reached.

BEFORE

- In the store, the ID is copied and typed into the contract form field by field.
- Online, every email address is accepted, including disposable ones.
- Applications through VPNs or data centers look like all the others.
- Nobody notices that one device has already filed several applications.

WITH PAPEROFFICE

- The online form checks the email address, and on REVIEW the application goes to review.
- The IP check reports VPN, Tor and data center, and the application compares the country with the address.
- Each application stores the visitor_id, so devices used several times stand out.
- In the store, an IDP Agent reads the ID from a photo, and the team checks the values against the source.

Example for illustration, the company and the process are made up. Check with your data protection officer which ID and device data you collect and how long you keep it.

05 · CHECKLIST

Ten points for your customer onboarding.

Go through these points with sales, IT and data protection. Each one can be checked in your own business.

- ☐ Every sign-up checks the email address before the account is activated.
- ☐ Your backend sends the customer's IP address to the API in the ip parameter.
- ☐ The country of the IP address is compared with the stated address.
- ☐ If a known account signs in from an unfamiliar device, your application asks for a second factor.
- ☐ For deletion requests, the path via POST /privacy/forget is documented.
- ☐ For REVIEW and REJECT, it is defined what happens: ask again, send to review or reject.
- ☐ VPN, Tor and data center are assessed separately, with a rule for each case.
- ☐ The visitor_id is stored with every account and every application.
- ☐ An IDP Agent reads ID documents, and the required fields are defined.
- ☐ Purpose, legal basis and retention period of device data are agreed with data protection.

06 · FREQUENTLY ASKED QUESTIONS

What teams want to know before they start.

Does PaperOffice check IDs biometrically?

PaperOffice works without face matching. An IDP Agent reads the fields of the ID document with their source location, and the other checks deliver signals on email, network and device. Your team decides whether an identity is confirmed.

What about people who use a VPN for good reasons?

A VPN is a signal that your rule weighs. The response separates VPN, proxy, Tor and data center and names the matching list in the type field. Addresses from blocklists also appear under is_vpn.

How do the checks get into our portal?

Via the REST API from your backend, via the fingerprint SDK with a **Publishable Key** bound to your domains, and via MCP. You upload ID documents into a workspace where an IDP Agent runs.

Where does the risk score come from?

From the email check: risk_score from 0 to 100, risk_level from MINIMAL to CRITICAL and the recommendation ACCEPT, REVIEW or REJECT. The device check delivers its own risk factors, such as a VPN or impossible travel speed.

Can I spot the same device behind several accounts?

Yes, if you store the visitor_id with every account. Then the same ID appears on several accounts. /fingerprint/similar finds devices with similar traits, /fingerprint/linked devices from the same network.

How do I handle deletion requests?

POST /privacy/forget deletes the device profile, links, history and alerts for an identifier in your organization. A block marker prevents the same identifier from being recorded again.

07 · HOW TO START

Check your next sign-up with real signals.

Create an account on app.paperoffice.ai, generate an API key under [API & Developer > API Keys](#) and check your first address with POST `/fakeemail/check`. Billing is pay as you go, details are on the pricing page.

Add the email check

Your sign-up form sends the address through your backend to `/fakeemail/check` and acts on the recommendation field.

Add IP and device

`/ip2location/full` for network and location, the fingerprint SDK for the `visitor_id`. Store both with the application.

Have IDs read

Create an IDP Agent with an ID template and let it run automatically after processing in the workspace for applications.

DATASHEETS ON THIS TOPIC

Fake Email Detectionpaperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf**VPN Detection**paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf**IP Location API**paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf**Device Fingerprint**paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing.pdf

MORE ON THIS TOPIC

Identity fraudpaperoffice.ai/en/solutions/risk/ai-identity-fraud-detection-prevention

MORE ON THIS TOPIC

paperoffice.ai/en/solutions/risk/ai-identity-fraud-detection-prevention

PRICING

paperoffice.ai/en/pricing

CONTACT

paperoffice.ai/en/contact