Put an end to fraud once and for all

with Veriff

Combat bad actors on multiple levels

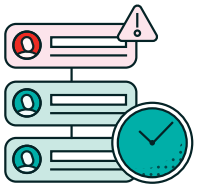
Veriff empowers online businesses to onboard and convert honest users fast while identifying and mitigating all kinds of fraud.

Greater transparency for maximum confidence

Veriff's fraud prevention layer works in the background to stop bad actors in their tracks.

Prevent multi-accounting

Automatically prevent the same users from opening multiple accounts, requesting multiple loans or abusing sign-up bonuses with Veriff's Velocity Abuse feature.



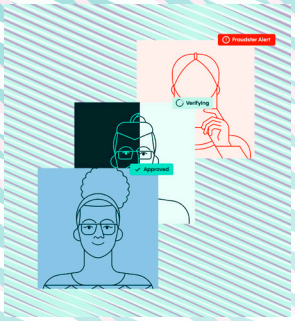
Agile fraud protection

Fraud trends change faster than code. Veriff's technology can create rules based on data points that either send verification sessions to manual review or decline them.

Leverage Veriff's data

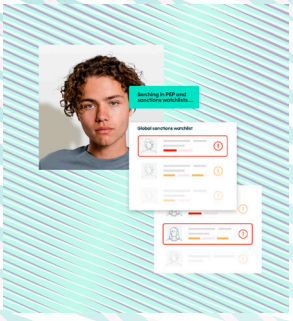
Build your own advanced and flexible anti-fraud flow based on device and network data points.

How does it work?



1. Device & network fingerprinting

Our comprehensive profile of raw data grants us free rein over exactly which pieces of information we decide to use and how.

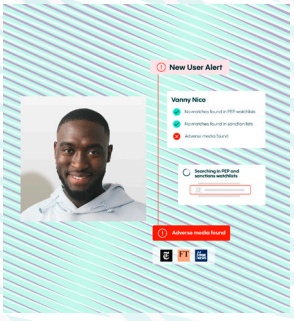


2. Crosslinking

Our fraud engine ingests thousands of data points and compares them to historical session data to identify any fraud patterns and trends.

3. Risk labels

Warning labels are generated to note potentially suspicious behavior in a verification session, like the use of a VPN or the user's document country being from a different time zone than their device network.



4. Face blocklisiting

The blocklist functions as a separate, customerspecific set of data, where Veriff can add endusers based on the extracted face embeddings. All incoming faces will be checked against that database and if there is a match, the session will be automatically declined.

VFFRAOPEN11/22E

Veriff's device and network fingerprinting solution

Technical Overview

Robust fraud detection technology

Veriff's Device and Network Fingerprinting technology has been a cornerstone of gathering technical information about end-users accessing our flow. Veriff uses raw technical information to combat fraud, specifically reoccurring fraud.

Device and Network Fingerprinting solution collects data from multiple layers

Passive (Requests from Servers)

- Passive TCP/IP stack insight
- Passive SSL/TLS handshake analysis
- HTTP client user-agent string analysis
- Round Trip Time and variance
- IP information: (ASN/ISP, location, hostname,timezone)
- Signatures analysis, insight and recognition
- Signatures and IP velocity
- Risk layer for signatures and IP/network (negative/gray lists)

Additional parameters:

- hardware
- local network
- fonts
- plugins
- WebGL
- WebRTC
- audio
- battery
- browser features
- network performance
- Device internal identifiers
- Device name
- Hardware (cpu, memory, storage, screen, sensors, audio)
- OS/Kernel details
- User installed apps details
- Uptime details
- Network detection (radio, host, macAddress, IPV4/IPV6 IP, connected AP info, DHCP details)
- Carrier information
- Process environment information
- Emulator/simulator detection
- Jailbraking and rooting detection

JavaScript (Requests from browsers, hybrid mobile applications)

- Tagging + Tag retrieval capabilities
- Private browsing detection

Mobile (Requests from iOS and Android native applications)

- Tagging + Tag retrieval capabilities

Device and Network Fingerprinting Solution also returns the following IP-related risks:

- Known proxies
- TOR exit nodes
- TOR servers
- Anonymizing VPN providers
- Servers distributing or running malware/spywar
- Is part of a hijacked netblock or a netblock controlled by a criminal organization
- Running a hostile web spider / web crawler
- Hosting a malicious bot or is part of a botnet. Includes brute-force crackers
- Hosting a spam bot
- Hosting an exploit finding bot or is running exploit scanning software
- Is datacenter or hosting company
- Servers flagged on DShield

Device location detection with Veriff

- Veriff's Device and Network Fingerprinting technology collects the end-user's IP address, forward it then to our clients.
- This can be used to determine the end-user's location at the time of ID capture, unless they are using a VPN.
- When faced with a VPN, Veriff's Device and Network Fingerprinting Solution will read the location that the end-user wants us to read.
- In this case, the IP/device location will be off, but the rest of the relevant device ID data will still be useful, regardless of the VPN.
- While we do collect the IP location, it can only be accurate enough to determine the city/region that the end-user is coming from.

Veriff does not gather GPS information or IMEI code as these would require us to ask for extensive permissions from the end-user.