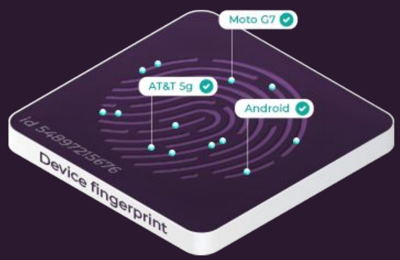
INCOGNIA

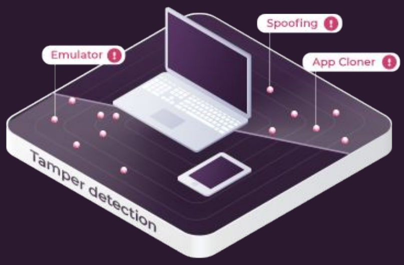
Prevent fraud without friction

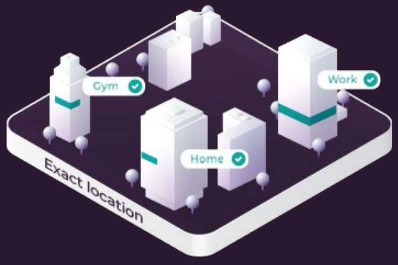
Provide a frictionless experience for good users, while protecting them with advanced account security

Integrated
Device Signal + Tamper detection + Location

Leveraging three integrated layers, Incognia delivers a strong risk and fraud signal while also enabling frictionless user verification and account security for trusted customers







Device Intelligence

Device ID (mobile + web)
Device + location fingerprint

Tamper Detection

Location tampering: GPS spoofing, VPN

Device tampering: Emulator, bot, root/jailbreak

App tampering: Manipulated app

Exact Location

<10 feet location accuracy, trusted location, suspicious location watchlist, location linked to device reset

Prevent fraud without friction

Fake accounts and ban evasion
Prevent promotion abuse and refund abuse, and maintain a safer platform for good users.

User verification and authentication
Seamlessly verify users to decrease abandonment and ensure a smooth customer experience, while providing strong account security.

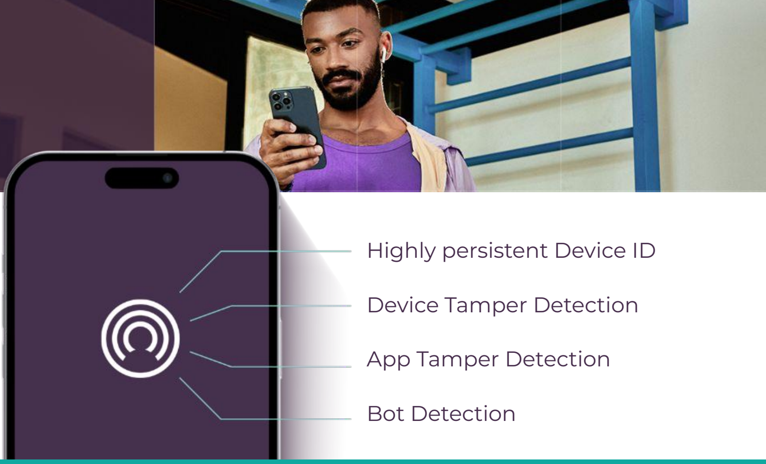
Account takeover
Protect seller banking credentials, personal information, and loyalty accounts without sacrificing user experience.

After moving to Incognia's frictionless solution, clients have:

85%	**reduction in promo abuse**
60%	**reduction in refund abuse**
93%	**reduction in collusion fraud**
93%	**of users authenticated without friction**

CCPA GDPR AICPA SOC 2

INCOGNIA



Device Intelligence

Incognia's device fingerprinting model leverages a wide range of independent attributes and fields, which create a modular, layered approach to identify device fingerprinting evasion.

Most device fingerprinting solutions:

Developed to identify regular user behavior for purposes such as advertising

Incognia's device fingerprint:

Purpose-built and continually enhanced to identify fraud and devices evading traditional fingerprinting.

Device ID
2.6x more performant
than the leading device fingerprint provider

Device ID
Over 99.9% accurate
device identification

Multi-layer Device Tamper Detection

For web and mobile

Device

Tampering Detection

Identify and recognize good users and fraudsters with 99.9% accuracy

- Emulator
- Modified OS location
- Root/Jailbreak
- Bot detection
- VPN/proxy/Incognito

+

App

Tampering Detection

Maintain trust in device signals with device, app, and location tampering detection

- Code injection
- App modification tools
- App properties mismatch

+

Location

Spoofing Detection

Location accuracy <10 ft becomes an identity signal, recognizing users across devices

- Mocked location
- Invalid velocity
- VPN/proxy

Exact Location

By fusing a variety of location signals, including GPS, WiFi, and Bluetooth, Incognia is able to identify the location of a device within a radius of 10 feet, transforming the data from a location to an identity signal.

Instant address verification

Rather than comparing PII to third party databases, Incognia checks the addresses used at onboarding against the location data of the user's device.

Trusted and suspicious locations

Analyzing user location behavior, Incognia identifies trusted locations, as well as suspicious locations where fraudulent activity is likely to occur. This location signal measures risk instantly, without introducing friction for good users.

CCPA GDPR AICPA SOC 2