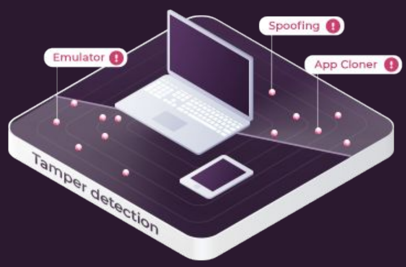
INCOGNIA

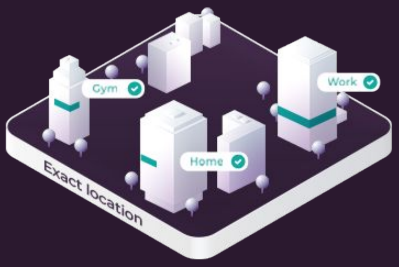
Incognia for Financial Services

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

Integrated
Location + Tamper detection + Device signal

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

Frictionless Authentication and ATO Prevention

By silently analyzing a device's characteristics and location behavior, legitimate customers are not exposed to frustrating authentication friction and bad actors are detected without the need for expensive 2FA processes.

Optimized location checks during sensitive transaction moments such as payments, transfers, and withdrawals ensure account security, without introducing any user friction.

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

Reduced new user abandonment by 84%

Reduced authentication costs by 30%

Authenticated 93% of users without friction

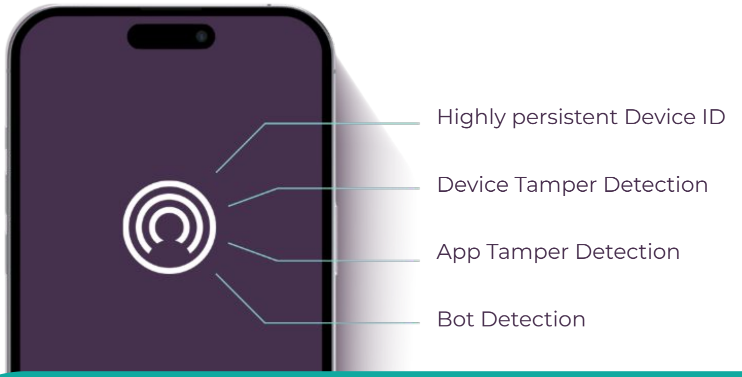
CCPA GDPR AICPA SOC 2

Device Intelligence

Incognia's device fingerprinting model leverages a wide range of independent attributes and fields, creating a modular, layered approach to identifying 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 detect devices evading traditional fingerprinting.



Device ID

2.6x more performant

than the leading device fingerprint provider

Over 99.9% accurate

device identification

Multi-layer Device Tamper Detection

For web and mobile

Device
Tampering Detection +

Device analysis to identify manipulation

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

App
Tampering Detection +

Analysis to detect app manipulation

- Code injection
- App modification tools
- App properties mismatch

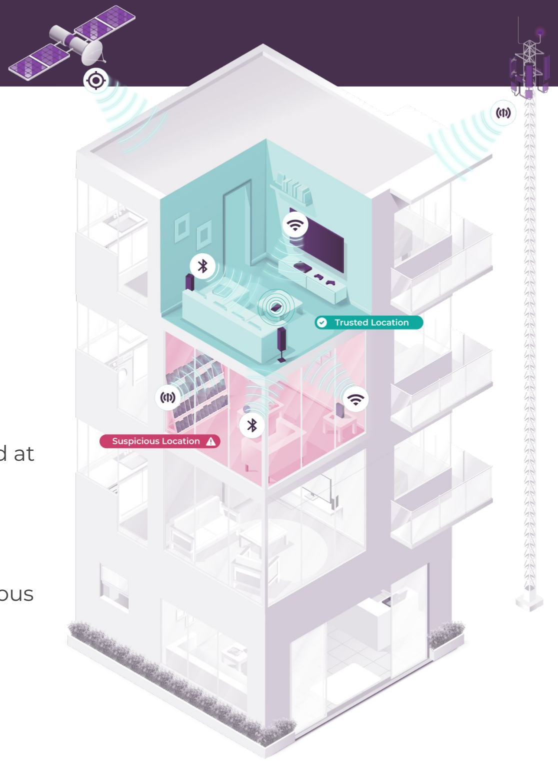
Location
Spoofing Detection

Combined device & location analysis for advanced tamper detection

- 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.