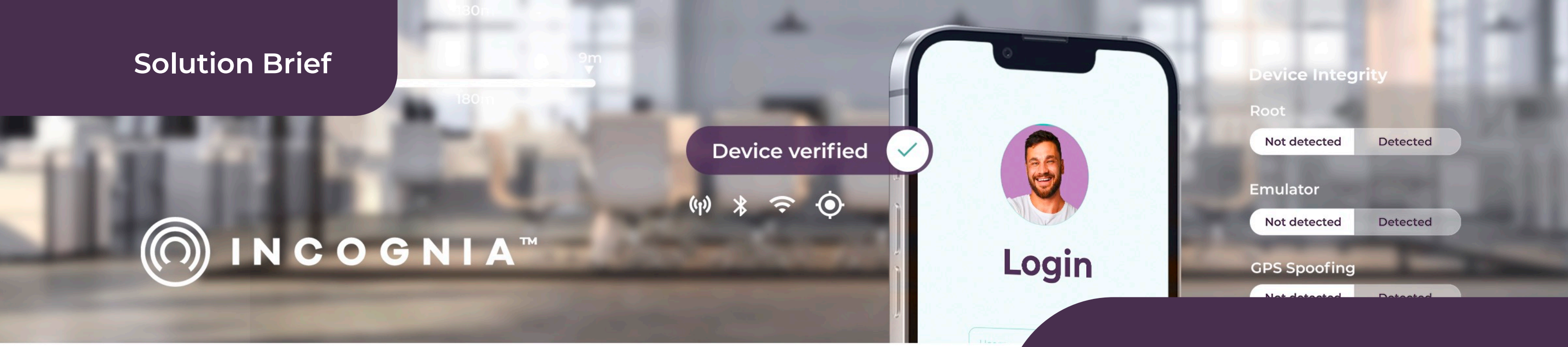
Solution Brief



Trusted Device Intelligence

Challenges

Mobile is one of the fastest-growing channels for organizations to interact with their customers. In financial services the growth of mobile transactions, using fintech or crypto apps, is attracting increased mobile fraud. The techniques used by fraudsters to commit fraud using their mobile devices include attempting account takeovers, impersonating users through stolen credentials or creating synthetic identities. Here are some examples of how fraudsters use their mobile devices to commit these types of fraud:

- **Use of Rooted or Jailbroken devices:** Fraudsters compromise mobile devices to attain privileged control over various subsystems of Android or iOS so that malware can easily breach the mobile security of the OS.
- **Use of Emulators:** fraudsters use emulators (standard tools to test mobile Apps from a computer) to easily manipulate the information they provide to apps and websites. "Emulator farms" have been observed where over 20 emulators were used to spoof over 16,000 compromised mobile devices.
- **Use of Apps from unauthorized app stores:** fraudsters get consumers to install modified or compromised versions of Apps from unauthorized app stores.
- **Multiple App reinstalls:** Fraudsters re-install apps several times in an attempt to hide their tracks by "cleaning up" their device memory and history.
- **Sharing the same device among different accounts** Fraudsters create many fake identities or login to multiple user accounts using the same device.
- **Sharing multiple devices on the same account:** Fraudsters use the same account with multiple devices to try to avoid having their device being traced.
- **Account Takeover simulating a device change:** Fraudsters try to take over accounts using a new device by phishing, smishing and performing SIM swapping frauds.

Organizations need updated tools to stop fraudsters from exploiting these vulnerabilities without increasing friction for good users.

Solution

Incognia Trusted Device Intelligence is an important overlay to standard device fingerprinting to enable the immediate recognition of trustworthy devices and deliver a frictionless experience for good users. This module enables enhanced mobile fraud prevention by using information from a user's device to detect use of emulators, rooted or jailbroken devices, and to detect when multiple devices are accessing the same account and multiple accounts are sharing the same device. The Trusted Device Intelligence solution module goes beyond traditional device fingerprinting in assessing not only the device integrity but also the device location to accurately assess risk whenever a new device attempts to login and access services. For trusted users this provides the opportunity for frictionless device change. The Trusted Device Intelligence module can be used in conjunction with Incognia Location Spoofing Detection and Address Validation modules.

Solution

Incognia Trusted Device Intelligence enables organizations to these mobile fraud vectors by recognizing trusted user's devices and location behavior. Untrusted devices can be blocked based on the Incognia Trusted Device Intelligence:

Device Integrity Check

Incognia detects device spoofing at the origin, and detects if the device has been rooted, jailbroken or if an emulator is in use.

Account Access Check

Incognia checks association between devices, re-installations and accounts, to assess suspicious device behavior.

Location Behavior Check

As an additional security layer, Incognia checks if the current device location matches the user's historical location behavior pattern.

Device Watchlist Check

Incognia creates Watchlists for fraudulent devices that have been reported as high risk and locations that have been associated with fraud. Incognia checks to see if the device is present on a Device or Location Watchlist.

Key Benefits

No Added Friction

Incognia Trusted Device Intelligence works automatically and silently in the background. No friction is added to the User Experience: Incognia helps discriminating between trusted users and fraudsters without requiring any additional steps from the user.

Validate Good User’s Trusted Device in Real Time

Incognia leverages device information captured from the user's mobile phone, as well as associated device behavior, to validate a trusted user device in milliseconds. Incognia provides a low risk / high risk assessment based on the user’s current device status, location and history. When a device is trusted, a low-risk assessment is provided. If the device fails any of these trust checks, a high-risk assessment is provided.

Enhance Fraud Detection From Untrusted Devices

Incognia detects fraud by performing device integrity checks, evaluating device/account behavior and by checking Watchlists for known bad devices. This enables customers to block untrusted devices during onboarding, login or transaction operations.

Prevent Account Takeover at Device Change

Incognia Trusted Device Intelligence solution goes beyond traditional device fingerprinting in assessing not only the device integrity but also the device location. This enables apps to accurately assess risk whenever a new device attempts to login and access services.. Most account takeover attacks are now a result of social engineering, phishing and SIM swaps but still, most Apps are using SMS as part of their new device authorization process, which is highly vulnerable to these attacks. Incognia leverages the device location to provide trusted users with an opportunity for secure and frictionless device change.

Enroll users with Zero Factor Authentication

Incognia’s advantages are not limited to assessing device trust. Incognia Zero Factor Authentication solution also, leverages privatized location identity signals to understand if the user behind the device is trusted.. This offers an extra layer of security during onboarding, login, device change and during other sensitive transaction processes.

How it Works

01

Native mobile apps compile Incognia’s SDK, which passively profiles the user’s device during onboarding, logins or transactions via the mobile app.

02

The Incognia SDK transmits the Device Information and location behavior to Incognia’s Back End.

03

Incognia responds in real time to the customer with a risk assessment , as well as the supporting evidence, such as device’s integrity and account -> device -> installation associations.

04

The Incognia SDK is deployed in over 150M devices. If the device has been previously seen by Incognia the history of the device can also be used to assess device risk.

How Incognia Detects Trusted Devices

Fraud Vector on Device	How
Device Rooting / Jailbreaking	Detect Rooting / Jailbreaking
Emulators	Detect Emulators
Sharing the same device on multiple accounts	Detect how many users accounts are accessed using the same device
App re-installs	Detect how many times app is reinstalled on the same device / account
Unauthorized App Stores	Check if the App has been downloaded from an official App Store
Sharing multiple devices on the same account	Detect how many devices log in to the same user account
ATO at Device Change	Detect if the new device is in a trusted location for the user

Key Capabilities

- Deliver Device Intelligence on rooted, jailbroken or emulated devices used by fraudsters to open new fraudulent accounts or to perform account takeovers and other fraudulent transactions.
- Deliver Device Intelligence about the behavior of the device associated with accounts. Detects if: the app has been re-installed multiple times, the same device is being used across multiple accounts, or an account is being accessed by multiple devices. These high risk devices can be blocked or further verification and/or authentication processes can be initiated based on suspicious activity.
- Deliver Device Intelligence based on device location. Incognia can provide a high risk assessment if the current device location deviates from the device's historical location pattern.
- Provide specialized Watchlists to alert customers to risky onboarding transactions. Incognia has analyzed the behavior of over 150 Million devices and developed Watchlists based on prior fraudulent behavior.
- If a device is found in these Watchlists, Incognia provides an "high-risk" alert and the suspicious device can be immediately blocked by the customer.

Key Features

Real-time validation of user trusted devices

- Supports iOS and Android mobile devices

Works in any geography

- Global address validation coverage

Highly accurate risk-assessments

- Device fingerprint and device integrity
- Behavior watchlist and network effect

Lightweight SDK

- 415 KB (Android)
- 1.5 MB (iOS)
- Battery usage: ~0.5% per day

Easy to integrate and use APIs & Webhook

- REST & JSON Response
- Average response time: 60 ms
- Low latency of the Incognia APIs
- Integration time: 1 hour

Use stand-alone or integrate to your risk-engine

Advanced technical support

- Open documentation
- API reference
- How-To Guides
- Developer Portal

Privacy and Security

- GDPR, CCPA and SOC 2 Compliant

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech and mCommerce companies, for increased mobile revenue and lower fraud losses. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns and is a key enabler for Zero-Factor Authentication. Deployed in over 150 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.