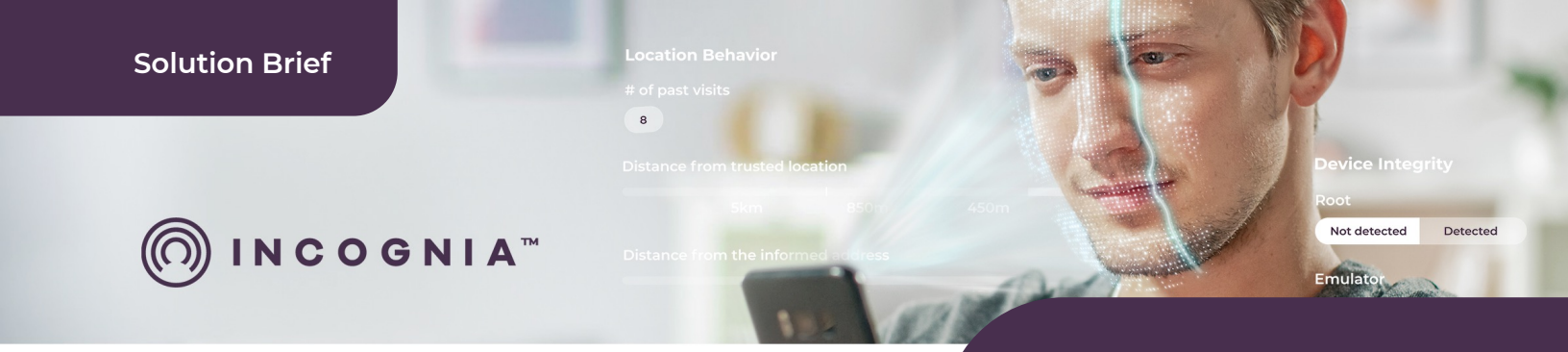
Solution Brief



INCOGNIA™

Location-based Liveness Spoofing Detection

Detecting use of Deepfake videos

Challenges

Fraudsters are creating online accounts using fake identities to take advantage of sign-up bonuses and to create “money mule” accounts for money laundering purposes.

To verify a new user’s identity on a mobile app, the onboarding process today typically involves taking a selfie and passing a biometric “liveness test”. Fraudsters are now using several techniques to spoof liveness to trick the selfie liveness detection algorithms. One common method is the use of facial images downloaded from the web to create deepfake videos . Several free or low cost software packages and Apps, such as Spark AR Studio, Mug Life and OBS Virtual Camera can be used to create effective deepfakes that can trick award winning liveness detection tools. Instructions and examples can be found on the dark web and even on YouTube.

There are two ways that these deepfakes can be used to spoof liveness.

- **Injection Attacks:** a deepfake video is injected in the onboarding app using an emulator, a rooted or jailbroken device
- **Presentation Attacks:** a deepfake video is played using another device and then is presented in front of the device with the onboarding app.

Organizations need effective tools to stop fraudsters from exploiting these weaknesses in biometric liveness detection during onboarding.

Solution

Incognia Location-based Liveness Spoofing Detection is an important overlay to biometric face recognition to enable the immediate recognition of biometric liveness spoofing attempts. Incognia enables enhanced mobile fraud prevention by using information from a user's device to detect use of emulators, rooted or jailbroken devices, that are the main ways fraudsters leverage deepfakes to spoof legitimate liveness detection apps. The Incognia Location-based Liveness Spoofing Detection solution module goes beyond traditional biometric systems and assesses the device integrity and also the device location to accurately determine risk whenever a user performs a selfie and submits a biometric proof of liveness. The Location-based Liveness Spoofing Detection module can be used in conjunction with Incognia Location Spoofing Detection and Address Validation modules.

Solution

Incognia Location-based Liveness Spoofing Detection enables organizations to block mobile fraud vectors by recognizing if a fraudster is trying to use a deepfake to spoof liveness in biometric systems during onboarding.

Deepfake Injection Attack

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

Deepfake Presentation Attack

Incognia checks association between devices, device location, 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 liveness spoofing and fraud. Incognia checks to see if the device is present on a Device or Location Watchlist.

Key Benefits

No Added Friction

Incognia Location-based Liveness Spoofing Detection works automatically and silently in the background. No friction is added to the user experience and Incognia is highly effective in recognizing trusted users and detecting fraudsters without requiring any additional steps from the user.

Validate Good User's Liveness 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 the Incognia trust checks, a high-risk assessment is provided.

Block Deepfakes, Biometric Liveness Spoofing and Enhance Fraud Detection From Untrusted Devices

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

Enroll Users With Zero-Factor Authentication

Incognia's advantages are not limited to detecting liveness spoofing at onboarding. Incognia's Zero-Factor Authentication solution also leverages location identity signals to understand if the user behind the device is trusted throughout the user journey. 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 integrate Incognia's SDK, which checks 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 200M 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 Liveness Spoofing

Liveness Spoofing Techniques	Detected by Incognia	Detection Methods
Deepfake is injected using a rooted or jailbroken device	Yes	• Device Integrity checks on OS • Incognia Device Watchlists
Deepfake is injected using emulators	Yes	• Emulator Detection
Deepfake using a presentation attack: User spoofs liveness from an "untrusted" location	Yes	• Detect the same device accessing multiple accounts • Detect device is in a different location • Incognia Location Watchlists • Incognia Device Watchlists

Key Capabilities

Detects biometric liveness spoofing

- Detects use of rooted, jailbroken or emulated devices used by fraudsters to open new fraudulent accounts or to perform account takeovers and other fraudulent transactions.
- Detects deviations in user location behavior and provides a high risk assessment if the current device location deviates from the device's historical location pattern.

Detects multiple app installs

- Detects high risk devices where 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.

Detects high risk devices

- Provides specialized Watchlists to alert on high risk onboarding transactions. Incognia has analyzed the behavior of over 200 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 app.

Key Features

Real-time validation of user trusted devices

- Supports iOS and Android mobile devices
- Works in any geography

Highly accurate risk-assessments

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

Use stand-alone or integrate to your risk-engine

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

Advanced technical support

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

Privacy and Security

- GDPR, CCPA and SOC II Level 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 200 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.