Solution Brief

INCOGNIA™

Global Mobile Address Validation

Challenges

In today's increasingly digital world, there are many cases when organizations need to determine & verify the address of their users. This is particularly important during the onboarding stage of the new customer journey. For Fintech and Financial institutions this is required by the KYC (Know Your Customers) and AML (Anti Money Laundering) regulations. Besides being a compliance requirement, verifying the address of users can also be a strong fraud signal. Fraudsters use stolen PII (Personal Identifiable Information) to impersonate legitimate customers, or create synthetic identities to commit fraud. By verifying the address of the user that is trying to onboard, organizations can comply with regulations while also fighting fraud attempts.

Existing legacy solutions, currently used by digital enterprises, are of two different types that leave the door open to fraud:

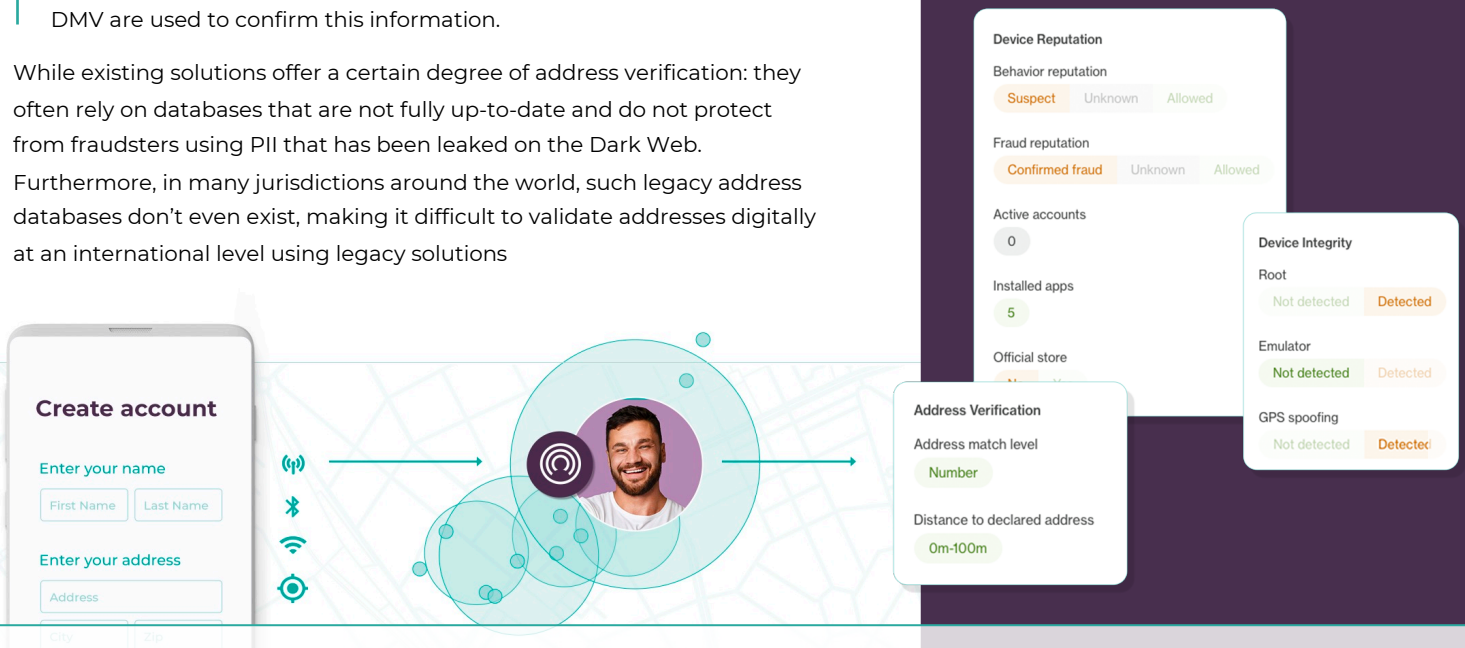
Address Validation
This checks that the address provided by the user physically exists. Services like the USPS and Google Maps can be used to check this box.

Proof Of Residence
This checks that the user currently lives (or has lived) at the address he/she provided. Usually government database services such as the DMV are used to confirm this information.

While existing solutions offer a certain degree of address verification: they often rely on databases that are not fully up-to-date and do not protect from fraudsters using PII that has been leaked on the Dark Web. Furthermore, in many jurisdictions around the world, such legacy address databases don't even exist, making it difficult to validate addresses digitally at an international level using legacy solutions

Solution

The Incognia solution for Global Mobile Address Validation uses Location Behavior and Device Intelligence to validate the address of the user. Using Incognia, mobile apps can determine the user location in real time and the distance from the address provided by the user. Since about 85% of accounts are opened from home (based on Incognia data), this is a strong signal that the user currently lives at this address. By checking the user provided address with the address validation service provided by Incognia, enterprises can support the KYC/AML compliance requirements while also defeating fraud attempts based on the use of leaked or stolen PII.



Key Benefits

Validate User's Address in Real Time

Incognia uses location information captured from the user's mobile phone to validate an address in real time in less than a second. Incognia provides a low risk / high risk assessment based on the distance of the user detected location vs. the address provided by the user. When the user is within a small distance from the provided location a low-risk assessment is provided, or if the user is a long distance from the stated location a high-risk assessment is provided.

It Works Everywhere – Globally

Legacy solutions mostly use database pings to verify addresses using public / private online address databases. However, in some International jurisdictions there may not be address databases available online. Even where address databases do exist, they may not be up to date and sometimes they may provide dated information.

Incognia Address Validation works everywhere, internationally in every country and region: it can help your KYC/AML efforts across the globe providing real time address information. Incognia Address Validation can be used either as a stand alone solution or in waterfall with legacy database ping solutions.

Enhance Fraud Detection

Incognia detects fraud by matching the user's physical, real-time location with the address provided during the onboarding process. Some fraudsters try to use stolen PII from the Dark Web to impersonate victims. Incognia can signal as "high risk" a transaction if the real location of the device used for the transaction is far away from the stated address. This enables customers to block the onboarding operation.

Improve Compliance with International Regulations

KYC and AML regulations require verifying the address of the users who are onboarding. Several financial authorities at international or national level have started recognizing the importance of geolocation in the KYC process to validate user addresses. The degree of implementation may vary by jurisdiction: in some places (Mexico CNBV) it has started to be a requirement in 2021, in others it is an accepted methodology (Brazil PLDFT), in others simply a suggested improvement for a robust CDD (Customer Due Diligence) process (International FATF).

Enroll users with Zero Factor Authentication

The Incognia advantages are not limited to the onboarding journey: after establishing the user address & location during onboarding, Incognia location behavior and device intelligence adds protection to login, device change and sensitive transaction processes leveraging Incognia Zero-Factor Authentication

How it Works

01

Users provide their address during onboarding via the mobile app

02

The Incognia mobile SDK sends the stated address together with device information (including GPS location) to the Incognia Back End.

03

Incognia provides the customer with a risk assessment in real time, and the evidence that supports the assessment, such as the user's distance from the stated address and details about the device's integrity.

04

The Incognia SDK is used by over 150M devices. If it's the first time that Incognia sees the device, only real-time location information is used to validate the address. If the device has been previously seen by Incognia also the location history of the device is also used to infer the user address.

Key Capabilities

- Detect distance from the physical user location and the address provided during the onboarding for KYC/AML workflows
- Deliver Device Intelligence on rooted, emulated, jailbroken devices used by fraudsters to open new fraudulent accounts
- Provide specialized watchlists to alert on risky onboarding transactions. Incognia has analyzed the behavior of over 150 Million devices and developed watchlists based on prior fraud behavior.
- Incognia maintains a watchlist based on devices previously associated with fraudulent activity, including devices accessing multiple accounts, emulator usage, and location spoofing.

Incognia Device Watchlist
Provide an high risk assessment if the device used for KYC has been previously detected in bad actions.

Incognia Location Watchlist
Provide an high risk assessment if the device location, has been detected with previous bad actions.

- 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 address using device location information

- Supports iOS and Android mobile devices

Works in any geography

- Global address validation coverage

Highly accurate risk-assessments

- Location fingerprint and location analytics
- 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.