INCOGNIA™

Mobile gaming app blocks fraudsters using location spoofing detection and trusted device intelligence

A mobile gaming app with over 70 million active users implements Incognia's location identity to stop fraudsters.

The Challenge

A leading social gaming mobile app provides multiplayer skill games, such as Poker, Rummi and Ludo. The app requires the users to share their location for two main reasons:

1. **Comply with regulations:** these types of online games are regulated and are only legal in some states / jurisdictions, so operators are required to have geofencing capabilities to allow/disallow players depending on the user's location.

2. **Combat player fraud:** one of the most pervasive fraud types seen by these online skill games is collusion between players that are playing at the same virtual table.

The existing mobile app geofencing capabilities, even if functional from a compliance perspective, were not effective in detecting players using location spoofing techniques to commit fraud or to play from unauthorized locations.. To create a fair and trusted environment, the mobile app has to ensure that players do not share cards or any type of information among themselves. **The product team needed a solution that could block fraudsters from colluding in the mobile gaming app.**

Background

In order to commit collusion fraud, bad actors use three different methods. While playing the game at the same virtual table, they are physically sitting near to each other, sharing cards and game data by:

1. Using **GPS Spoofing** to mask their actual location
2. Logging into **multiple accounts** from one device
3. Logging into the same account from **multiple devices**

To support a fair and trusted gaming environment, **the company needed a scalable GPS spoofing detection and device intelligence solution.**

The Solution

The product team attempted to build their own geolocation solution to detect user collusion and other location spoofing attempts, but it proved ineffective and costly to build and maintain.

For these reasons, the company chose to test the Incognia Location Spoofing Detection and Trusted Device Intelligence solutions. The Incognia's SDK uses

Company Profile

- Social gaming mobile app
- Founded in 2018
- 70M+ active users
- 100+ skill games

Results

- **94.3%** of accounts verified when location permission enabled

- **5** different watchlists generated with the suspicious device and location information collected by Incognia

- **50K+** total suspicious accounts (~1.8%) detected from 5 watchlists

the sensors on a mobile device to determine the real-time location of a user with precision of up to 10 feet (~3 meters) and also perform device integrity and device behavior checks, including detecting signs of GPS spoofing. For this customer, Incognia created five custom fraud watchlists:

Fraud Watchlists

Location Spoofing: accounts associated with spoofed location events

Devices With Multiple Accounts: accounts accessed by a device that also accessed at least 4 other different accounts

Accounts Accessed by Multiple Devices: accounts accessed by at least 4 different devices

Number of Installations: accounts that have at least 6 different installations associated with it

Suspicious Location: accounts related to a device that generated location events in a suspicious location (with more than 20 devices related to it)

Incognia's API delivers an immediate LOW, HIGH or UNKNOWN risk assessment, including all associated evidence, enabling the customer to make informed decisions on users at various sensitive moments within the gaming app. No PII (Personal Identifiable Information) is collected and the user's location information is handled by Incognia with the highest degree of privacy, in a way that is compliant with international privacy regulations including GDPR, and CCPA.

Incognia Evaluation

After the Incognia SDK was integrated into the app, Incognia analyzed 30 days of data collected from over 3.1 million gaming users across various types of devices and locations.

For the users that granted location permissions to the app, Incognia was able to deliver a risk assessment (low / high) for 94.3% of users. Out of over 3.1 million accounts analyzed during the evaluation, Incognia identified the following:

- **5K+**accounts flagged for **GPS Spoofing**
- **13K+** accounts accessed by **suspicious** devices
- **1K+** accounts accessed by **four or more devices**
- **30K+** accounts had **six or more installations**

- **400+** suspicious **locations**
- **10K+** accounts associated with **suspicious locations**
- **50K+** suspicious accounts total detected from **five watchlists**

Using Incognia, the social gaming company detected and stopped systematic collusion fraud by identifying cases of GPS spoofing, suspicious accounts, suspicious devices and suspicious locations.

Based on the increased blocking of fraudsters, Incognia was selected by the product team and was rolled out to all 70M users of the gaming app.

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.