

Case Study

Fintech achieves 80% reduction in account takeover (ATO) and 90% cost reduction on mobile

A challenger bank, with two million customers, drastically reduced the number of fraudulent logins and provided frictionless authentication for 93% of legitimate users, using Incognia.

The Challenge

A high growth fintech app became a big target for fraud via a **social engineering attack to their digital wallet** through social media. In possession of legitimate users' data, fraudsters logged into the app to commit fraudulent transactions, resulting in increasing financial losses and negatively impacting the customers, mainly medium and low incomes, and the company's brand reputation.

The Solution

The fintech needed to adopt a solution that could **detect and reduce the number of fraudulent logins** in its digital wallet and, at the same time, **keep the user experience optimized** for legitimate users. That is why they chose to integrate the Incognia location identity for mobile for risk-based authentication solution to their digital wallet. The primary goal was to deliver a friction-free experience for trusted users and require additional risk-based authentication steps for suspicious logins, to reduce the number of fraudulent logins.

Background

From January to May 2021, Incognia analyzed more than **72 million login attempts from over 1.3 million users** on the fintech mobile app. For this mobile app, over **83% of users have location permissions enabled**, resulting from a clear

Company Profile

- Challenger bank
- \$600M/yr in transactions (2019)
- 200M users
- 14M logins/month (approx)
- iOS and Android Apps
- 83% opt-in for location



Results

- 80% reduction in ATO
- 90% reduction in ATO costs
- 93% users frictionless authentication
- 0.0013% false positive rate
- 480% ROI

opt-in flow in the first user interaction with the app. This high opt-in rate contributed to the effectiveness and speed of results from their deployment of Incognia, enabling recognition of a high percentage of trusted users and a very low false positive rate of 0.0013%. After the integration of the Incognia SDK and risk scoring APIs the fintech saw a dramatic reduction in the number of account takeovers and associated fraud.

With Incognia the fintech was able to recognize trusted users, with a very low positive rate of 0.0013%, and remove the need for extra authentication steps for the vast majority of logins, except those identified by Incognia as high risk.

How does Incognia work?

The Incognia SDK collects anonymous location data from the mobile device, through its proprietary location technology, using data from GPS, WiFi, cellular and Bluetooth sensors. Each user's location behavior pattern is unique, and made up of frequently visited locations or trusted locations. Whenever a user tries to log in, from a new or existing device Incognia assesses the user's current location behavior with their historical location pattern. According to Incognia network data, 90% of legitimate user logins and 89% of sessions on bank and fintech apps occur from a trusted location.

For each login attempt, Incognia provides a risk score through the Incognia APIs, together with a confidence rating based on the correlation of current and historical user location behavior and device intelligence data. Incognia maintains a behavior watchlist, which is a device database containing a history of fraudulent actions and associated devices including devices accessing multiple accounts or using emulators or spoofing. The Incognia watchlist leverages the Incognia network of close to 100 million devices and enables the detection of not only devices used for fraud, but also locations associated with fraud, such as fraud farms.

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 costs. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns. Deployed in over 100 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.

www.incognia.com

