Persistent Fraud Attack Stopped With App Tampering & Factory Reset Detection Features

A large delivery platform implemented Incognia's active identity assurance signal to identify multi-accounting scams used by bad-acting couriers to steal from customers.

The Challenge

A large food delivery platform was suffering from a new social engineering attack in which bad-acting couriers were stealing cash payments from customers. The app took action by closing all implicated accounts and flagging the involved devices, however, customer support continued to receive complaints. In an attempt to retain customers, the app was issuing refunds which was driving up its total fraud losses.

The Solution

The risk team hypothesized that the apps device identification solution was being bypassed, enabling the bad actors to use the same device to open new accounts and continue defrauding the app.

Familiar with the characteristics of the attack, the Incognia team uncovered that the fraudsters were using the factory reset feature and running tampered versions of the courier application in order to bypass the outdated device identity feature. These techniques enabled bad actors to use the same device to open multiple accounts and even use app cloning tools to run multiple installations of the app on one device.

Incognia implemented its Suspicious Location feature to re-identify devices that had been involved in the scam by their location behavior and device attributes. By detecting the clusters of suspicious devices, apps are able to preemptively block devices based on their precise location, even if the device appears to be unique.

With this solution in place, the food delivery app receives real-time alerts when:

- Clusters of high-risk devices are concentrated in a precise location, like a small store or apartment
- A device connects from a precise location previously associated with risky app installations
- A device connects from a precise location that has been previously associated with confirmed fraudulent activity

Company Profile

- Leading food delivery platform globally
- 750,000 users on the courier application

Results

- 51% reduction in fake account creation
- 5% reduction in total fraud losses
- Prevent repeat offenders from bypassing device identification

This location-based approach is much less susceptible to factory resets or other app tampering techniques typically used to bypass device identity. When a device is reset and reinstalls the application, Incognia will detect the location of the device that is reinstalling it. If, for example, the number of installations occurring in that location exceeds a pre-defined threshold configurable by the client, then all the devices connecting from that location can be placed on a watchlist.

This rule enabled the delivery platform to track bad actors based on a pattern of location behavior. Once received client-side, the Incognia risk assessment and the associated evidence can be used flexibly to trigger blocklisting, a step-up security challenge, or outright rejection of the account creation, login attempt, or transaction.

High Risk
Suspicious location linked to multiple app installations
Low Risk
Good user

Conclusion

Incognia's cutting-edge fraud prevention technology was able to track and block repeat offenders. Its Suspicious Locations feature directly reduced fake account creation on the courier application by 51%, representing at 5% of the platform's total fraud losses.

> "Incognia has a solid solution and top notch post-sales support. Incognia is helping us identify systematic fraudulent behavior by providing a more reliable device identity solution."
>
> Global Head of Operations
> See the full review on G2

About Incognia

Incognia is the innovator in location identity solutions that deliver cutting-edge user verification and account security across the digital journey. Leveraging over a decade of expertise in location technology, Incognia's novel approach provides frictionless experiences using device intelligence and the most precise location data available. Incognia enables customizable risk analysis and actionable insights from day one that empower consumer businesses to prevent fraud, protect users and build customer trust.