SHIELD

SHIELD for Mobility Platforms

SHIELD's Device-First Fraud Intelligence platform identifies the root of fraud with the **SHIELD Device ID** and actionable **Fraud Intelligence**, helping ride-hailing & mobility platforms stay ahead of sophisticated complex fraud threats while safeguarding users and drivers.

Trusted by

inDrive careem ROUTE ... and more

"inDrive is dedicated to fighting injustice and upholding transparency and fairness in the mobility and transportation space. Our partnership with SHIELD empowers us to stay true to our mission of helping people, ensuring the highest standards of trust and fairness for all while maintaining our rapid pace of growth."

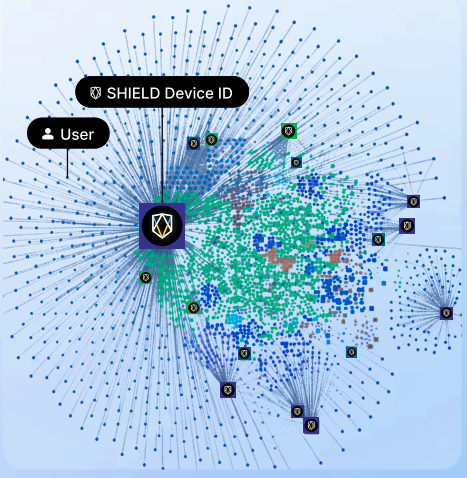
Arsen Tomsky
CEO & Founder, inDrive

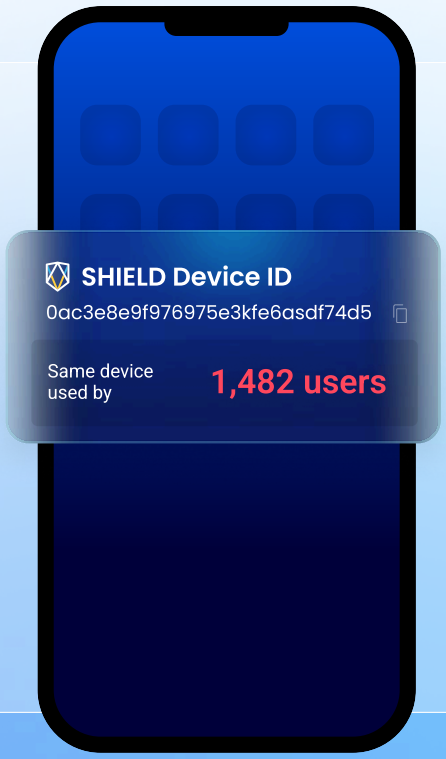
Our Solution

Plug-and-Play | No Additional Codes | No PII Required

SHIELD Device ID

persistently identifies the root of fraud & fake accounts >99.9% accuracy





SHIELD Fraud Intelligence

real-time actionable insights into fraudulent activity

20+ Configurable Risk Signals

App Cloner — Low / High
Auto-Clicker — Low / High
GPS Spoofer — Low / High
Emulator — Low / High
Device Masking — Low / High

... and more

Use Cases

Eliminate Driver & Passenger Collusion

What is Driver & Passenger Collusion?

Fraudsters create multiple fake driver and passenger accounts at scale with malicious tools, using them to exploit ride-hailing systems and gain unfair advantages for their benefit. This could include fare manipulation, fake rides, location spoofing, artificial surge pricing, and more.

Curb Fake Rides

Colluding fraudsters complete trips without ever transporting a real passenger. This is often done to exploit the system for bonuses, rewards, or artificially inflating earnings.

End Location Spoofing

Dishonest drivers use GPS spoofers to appear closer to passengers, disadvantaging honest drivers, increasing wait times, and potentially compromising rider safety.

Stop Artificial Surge Pricing

Fraud syndicates manipulate demand by combining fake accounts and GPS spoofers to create artificial fare surges in specific locations, driving up prices for their own benefit.

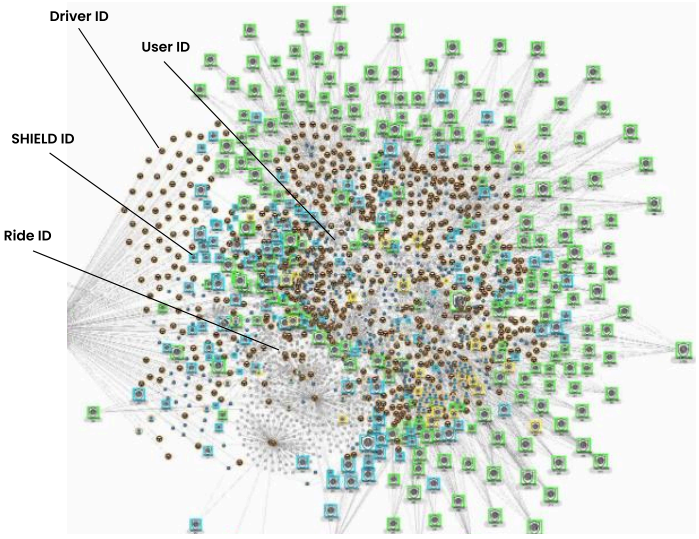
SHIELD Fraud Intelligence

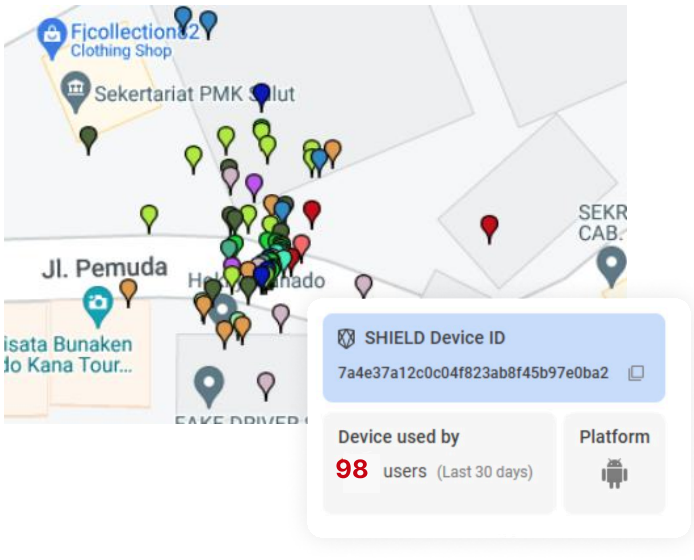
GPS Spoofers
App Cloners Running
Emulator Running
Suspicious Factory Reset
Jailbroken Devices
Tampered apps

How it Works

Fraudsters typically use a single device to create multiple driver and user accounts at scale. They exploit stolen identities, tampered apps, app cloners, auto-clickers, and emulators to carry out their schemes. By controlling both driver and user accounts, they manipulate prices and monopolize jobs.

SHIELD identifies interconnected accounts originating from the same device, detecting complex fraud clusters and stopping coordinated attacks. In one instance, we uncovered a cluster of **98 driver and users linked to a single device**, within a 5 metre radius. Further investigation revealed these drivers had shared multiple rides within a single day, which was highly suspicious.





Use Cases

Stop Location Spoofing

What is Location Spoofing?

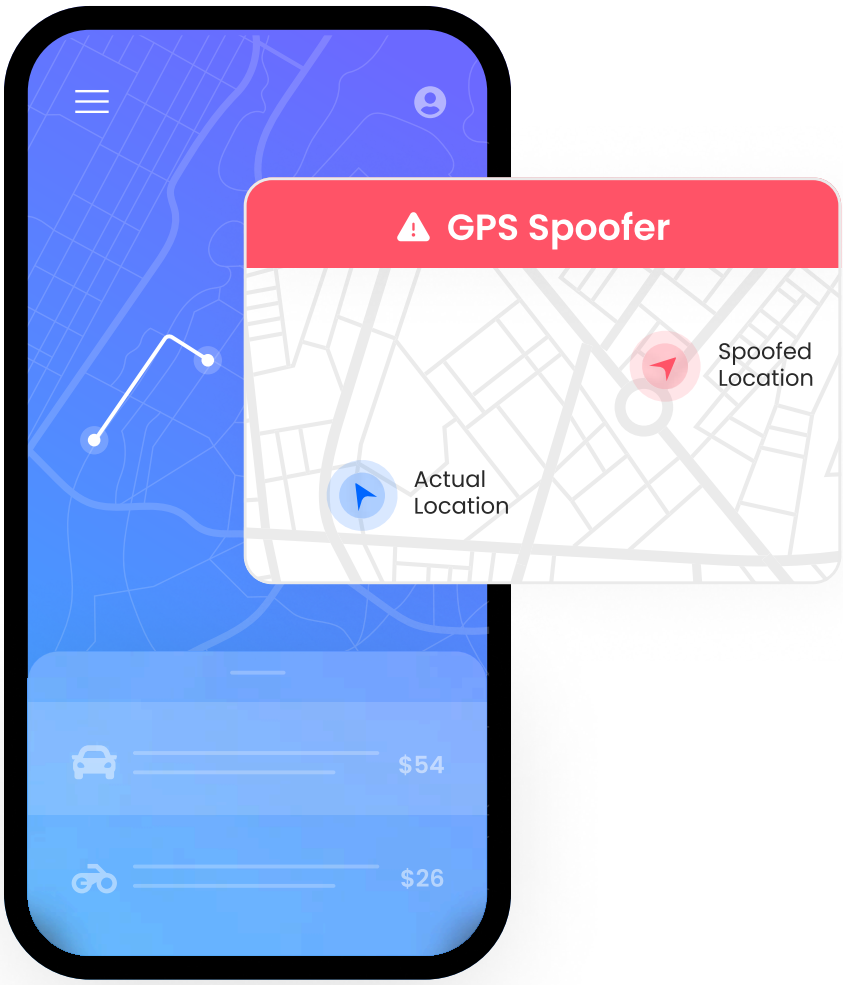
Location spoofing occurs when drivers falsify their GPS location using unauthorized software or techniques. This disrupts the platform's operations, allowing drivers to manipulate pricing, avoid traffic regulations, or falsify trip information. Spoofed locations can lead to revenue loss, degraded service quality, and a breakdown in trust between users and the platform.

Stop Driver Syndicates

Driver syndicates can exploit ride-hailing platforms to inflate earnings through coordinated fraud. By stopping location spoofing, you ensure fair competition among drivers, resulting in a more transparent and honest ecosystem.

Provide Safe & Trusted User Experiences

Safeguard users from fraudulent drivers and ensure accurate trip details, pricing, and reliability. This strengthens trust between your platform and your users customers, creating a secure and transparent experience.



Use Cases

End Referral & Promo Abuse

What is Referral & Promo Abuse?

Fraudsters can create many fake accounts to exploit new-user signup and referral codes. This type of fraud distorts the platform's marketing efforts, leading to significant revenue losses and reduced effectiveness of genuine referral programs.

SHIELD Fraud Intelligence

App Cloner Running
Emulator Running
Suspicious Factory Reset
Jailbroken Devices
Tampered apps
Auto-clickers

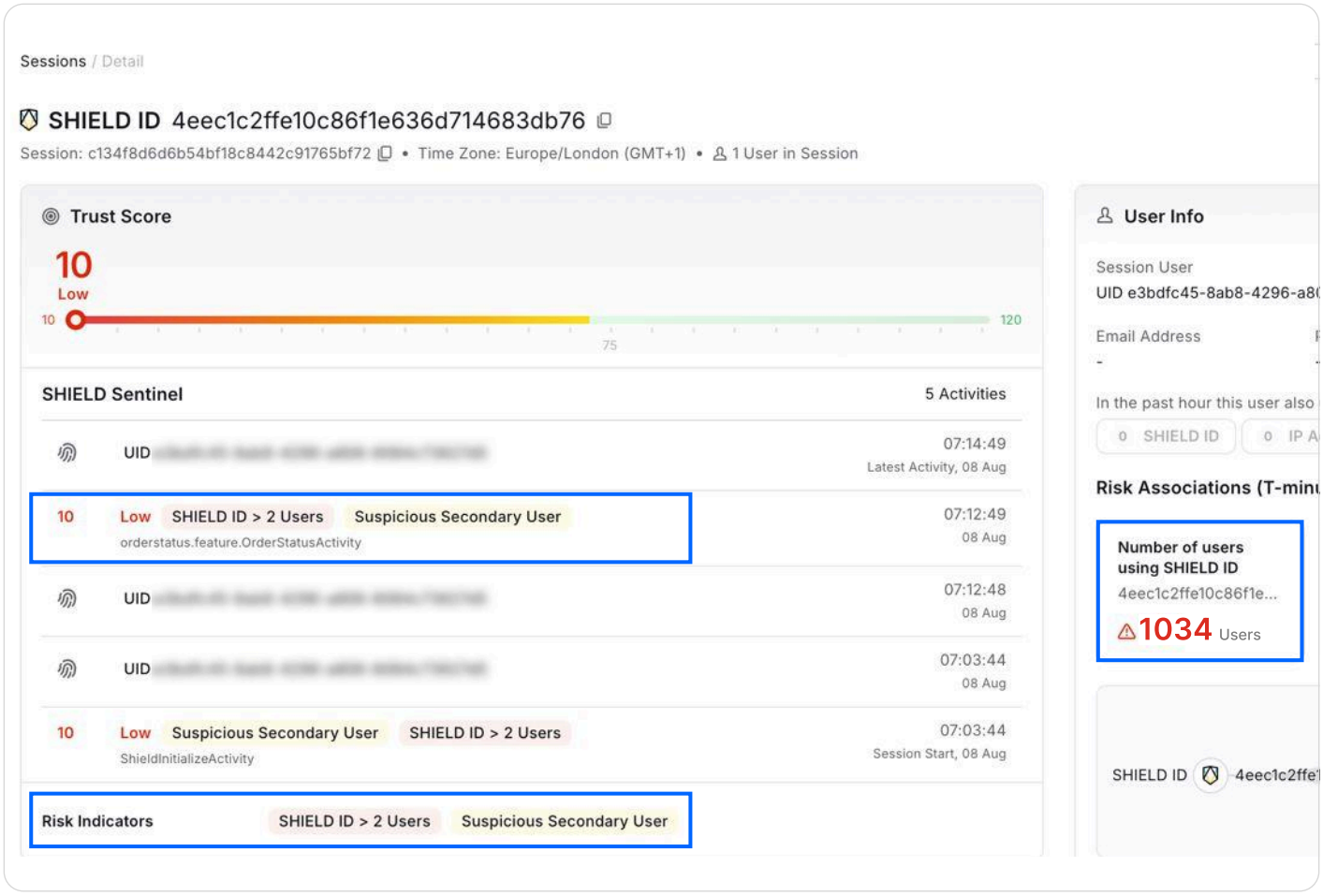
How it Works

Fraudsters create multiple accounts at scale with the help of stolen identities, tampered apps, app cloners, and emulators.

Typically, they use fake accounts to:

- Take advantage of new user signup bonuses
- Exploit referral codes by referring accounts controlled by themselves
- Redeem free rides or promo codes multiple times with different accounts

SHIELD identifies devices linked to multiple user accounts with the SHIELD Device ID, and detects tools used by fraudsters to automate and scale this process.



*All data has been randomnized