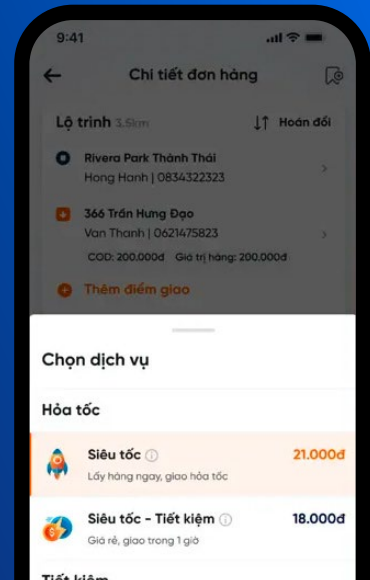


Case Study

Ahamove Cuts Incentive Fraud by 97% with SHIELD's Device Intelligence



"We used to rely on booking anomalies to spot fraud. By then, it was already too late. With SHIELD, we've shifted from reactive damage control to proactive fraud prevention. Their real-time device intelligence helps us stop fake accounts and GPS spoofers at the source. It's like having a full fraud team, without needing to build one ourselves."

Thuc Nguyen Canh
VP of Engineering, Ahamove

Key Takeaways



97% Reduction in fraudulent incentive payouts



99% Detection accuracy against GPS spoofing



3X Boost in operational efficiency by reducing manual fraud workloads

When Rewards Become Vulnerabilities

Part of Ahamove's business model is a reward-driven approach that incentivizes its delivery drivers with performance-based compensation. While this approach encourages productivity and engagement, it also creates opportunities for fraud. Drivers seeking to maximize rewards could exploit Ahamove's system using tools like GPS spoofers and shared accounts.

Key Fraud Tactics:

- Account Sharing Across Multiple Users**
 One driver account was shared across multiple individuals, allowing fraudsters to collectively fulfill more orders and climb the rewards leaderboard unfairly. This manipulation of the incentive system led to excessive, undeserved payouts.
- GPS Spoofing to Game Time-Based Incentives**
 Some fraudulent drivers used GPS spoofing tools to falsify their location data, making it appear as though they had reached delivery destinations ahead of schedule. This allowed them to meet strict delivery targets and qualify for performance-based incentives,

Customer Profile

Ahamove is Vietnam's leading on-demand logistics platform. They connect thousands of businesses and users with delivery partners to enable fast, reliable, and affordable fulfillment across urban centers.

Industry

Mobility & Delivery

Region

Vietnam

tricking the system into thinking they had reached a recipient earlier than they had. This tactic allowed them to meet delivery targets—earning rewards at the expense of service quality.

Without a dedicated fraud team in place, Ahamove had limited visibility into these behaviors. Their only line of defense was to analyze past data, often after fraudulent activity had already caused financial and reputational damage. As a result, sophisticated fraud schemes went undetected, skewing performance metrics, inflating incentive payouts, and undermining trust in the platform.

Driving Real Impact

To address these escalating threats, Ahamove partnered with SHIELD to embed real-time fraud detection as its first line of defense. With limited internal resources dedicated to combating fraud, Ahamove needed a solution that could offload the burden from its engineering and operations teams, providing effective, scalable protection with minimal manual intervention and maximum coverage.

SHIELD's device-first fraud intelligence platform filled that gap. With the SHIELD Device ID and actionable fraud insights, Ahamove gained instant visibility into suspicious behavior and the tools used to commit fraud.

How SHIELD Helped:

- **Prevented Account Sharing**
Ahamove used the SHIELD Device ID to spot when one driver account was being accessed by multiple devices

– a clear sign of account sharing. Since SHIELD's Device ID persistently and uniquely identifies every device on the platform, even after factory resets, Ahamove could stop drivers from gaming their rewards systems.

- **Blocked GPS Spoofing Instantly**

SHIELD detects location spoofing in real time, preventing drivers from manipulating delivery times to meet incentive goals. Fraudulent attempts to fake delivery times were automatically flagged with SHIELD's Fraud Intelligence, preserving the reliability of time-based incentives.

- **Automated Fraud Management**

Without expanding headcount, Ahamove gained real-time fraud detection and response capabilities. SHIELD slashed manual review time and restored the accuracy of driver performance metrics, allowing engineering teams to focus on growth instead of investigation.

The Road Ahead

By partnering with SHIELD, Ahamove transformed its fraud management strategy, shifting from a reactive posture to a proactive defense. Despite lacking a dedicated fraud team, Ahamove scaled its fraud detection capabilities through SHIELD's operationally efficient solution. With real-time signals and the SHIELD Device ID, the company now detects suspicious behavior before it impacts operations. This has strengthened the integrity of its incentive programs, optimized delivery operations, and rebuilt trust across its platform, establishing a strong foundation for sustainable, fraud-resilient growth.

SHIELD is a device-first fraud intelligence platform that helps digital businesses worldwide eliminate fake accounts and stop all fraudulent activity.

Powered by SHIELD AI, we identify the root of fraud with the global standard for device identification (SHIELD Device ID) and actionable fraud intelligence, empowering businesses to stay ahead of new and unknown fraud threats.

We are trusted by global unicorns like inDrive, Alibaba, Swiggy, Meesho, TrueMoney, and more. With offices in San Francisco, London, Berlin, Jakarta, Bengaluru, Beijing, and Singapore, we are rapidly achieving our mission – eliminating unfairness to enable trust for the world.

For more information, visit shield.com.

