SHIELD

SHIELD for E-Wallets & Superapps

SHIELD's Device-First Fraud Intelligence platform identifies the root of fraud with the **SHIELD Device ID** and actionable **Fraud Intelligence**, helping e-wallet platforms protect user information and stay ahead of sophisticated fraud threats.

Trusted by

truemoney maya ubank FE CREDIT WINK ZIGI Guavapay ... and more

"The perfect partner for us has to be able to scale alongside TrueMoney, possess strong technical expertise in mobile wallets, and the agility to stay ahead of both fraudsters' and consumers' constantly changing behaviors. SHIELD ticks all of these boxes."

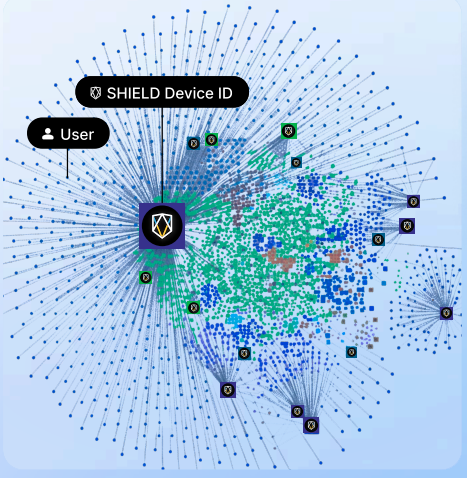
Monsinee Nakapanant
Co-President, Ascend Money

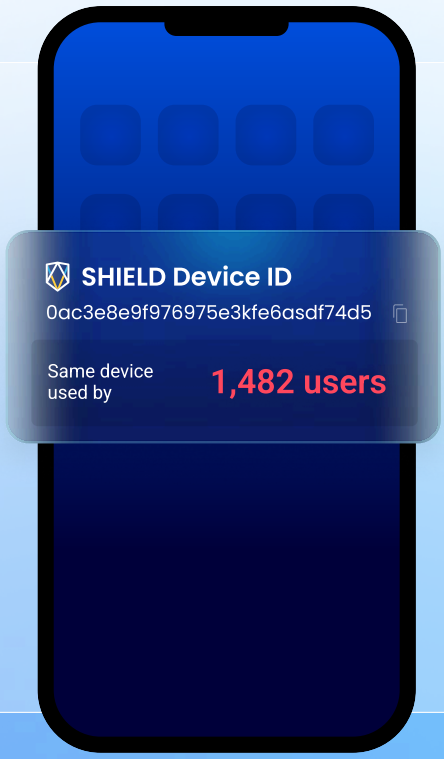
Our Solution

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

SHIELD Device ID

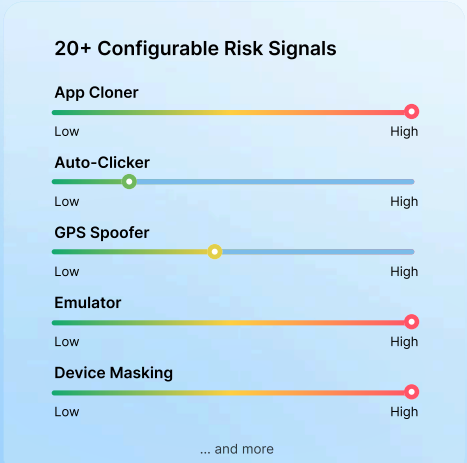
persistently identifies the root of fraud & fake accounts >99.9% accuracy





SHIELD Fraud Intelligence

real-time actionable insights into fraudulent activity



Use Cases

Eliminate Promo & Incentive Abuse

What is Promo & Incentive Abuse?

Fraudsters can create many fake accounts to exploit new-user signup and referral codes. To create these fake accounts, fraudsters can use stolen identities and fake IDs to bypass KYC checks. This causes **inflated growth numbers**, **lost revenue & trust**, and **skews marketing analytics** on the success of user campaigns.

Exploiting New-User Signups

Prevent fraudsters from exploiting promotions targeted at new users with fake accounts to claim rewards (e.g. free cashback) multiple times.

Colluding & Abusing Cashback Programs

Stop users and merchants from teaming up to fake purchases. Users pay with points, get cashback and split earnings, while merchants reimburse users and avoid fees.

SHIELD Fraud Intelligence

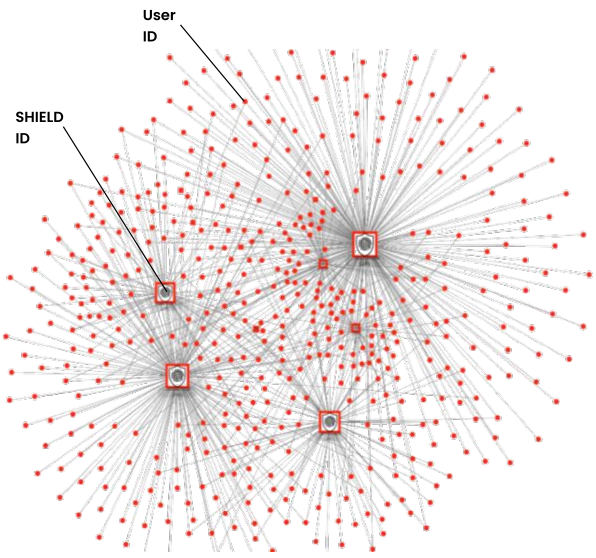
App Cloner Running
Emulator Running
Suspicious Factory Reset
Jailbroken Devices
Tampered apps
Auto-clickers

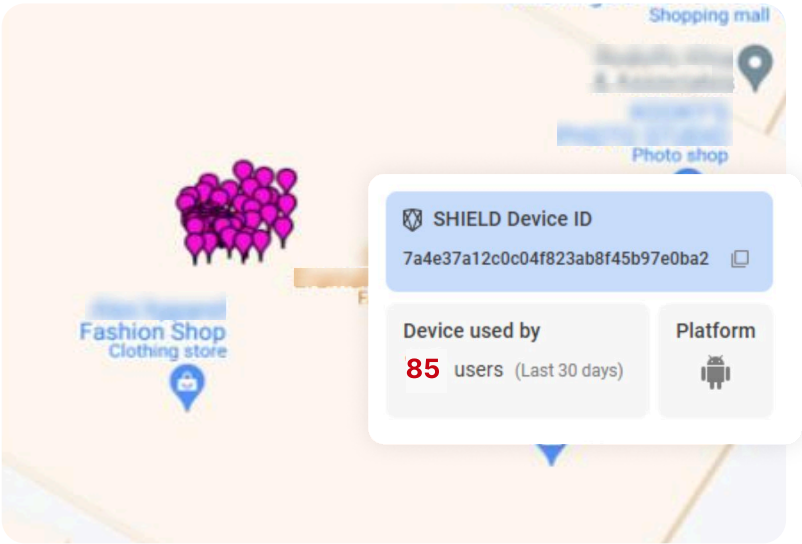
How it Works

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
- Collude with merchants to complete transactions and earn rewards

SHIELD persistently identifies devices linked to multiple user accounts with the **SHIELD Device ID**. SHIELD's **actionable fraud intelligence** exposes tools and techniques used to create fake accounts, like app cloners and emulators. Combined with **trusted location**, we pinpoint fraud hotspots and help you uncover the true scale of fraud.





All data has been randomnized

Use Cases

Stop Account Takeover Fraud

Accessibility Services Abuse & Social Engineering

What is Account Takeover Fraud?

Account takeover fraud (ATO) happens when a fraudster gains access to the victim's login credentials to steal funds or information. Once in, fraudsters can steal funds, conduct unauthorized trades, and even use the account to launder money.

01

Accessibility Services Abuse

Victims unknowingly download and grant malicious apps accessibility permissions. This allows fraudsters to gain control of their device, stealing data, keystrokes, OTPs and more.

02

Social Engineering

Fraudsters impersonate or pretend to be customer support or successful traders to trick the user into revealing sensitive information or transferring crypto to fraudulent accounts and wallets.

SHIELD Device ID

Identify sudden new devices accessing accounts with good history, from different locations - often a sign of ATOs.

SHIELD Fraud Intelligence

Detect malicious behaviour, including screen-sharing tools, auto-clickers, and device masking tools - usually signs that accessibility services abuse is taking place.

Passive Biometrics

Leverage data from device sensors and user interactions to identify anomalies like unusual device orientation, fast swiping, and unnatural keystrokes.

Use Cases

Stop Location Spoofing & Money Mules

What is Location Spoofing & Money Muling?

Fraudsters spoof their location to evade detection, accessing user accounts from alternative locations or to operate money mule accounts. AML regulations also often restrict transactions from high-risk areas. Criminals bypass these sanctions with location spoofing. E-wallets that unknowingly process transactions from mule accounts or unauthorized locations risk violating AML regulations and facing penalties.

Provide Frictionless User Experiences

SHIELD combines **trusted location** intelligence with persistent device insights to identify trusted users. Save on OTP costs and reduce the need for additional 2FA steps - required only when suspicious device behaviour is detected.

Identify High-Risk Activity & Stay Compliant

Significantly reduce false positives with real-time fraud monitoring. Leverage **trusted location** to stop activity from unauthorised locations, instances of impossible travel, and sanction lists. Stay in line with regulatory compliance.

Supercharge Mule Account Detection with Risk AI Models

2x your mule detection accuracy and enhance existing data models with actionable fraud intelligence. Eliminate fake accounts with SHIELD's persistent device IDs, built to withstand factory resets and advance tampering.