SHIELD

SHIELD for Digital Assets Platforms

SHIELD's Device-First Fraud Intelligence platform identifies the root of fraud with the **SHIELD Device ID** and actionable **Fraud Intelligence**, helping crypto & trading platforms stay ahead of sophisticated complex fraud threats while frictionlessly onboarding more users.

Trusted by

BTSE maya treasury HomeBroker tazapay ... and more

"Treasury is committed to supporting Indonesians in achieving their personal finance goals through the democratization of gold ownership. Our partnership with SHIELD helps us ensure our users are safe from fraud and can enjoy peace of mind on their financial journeys."

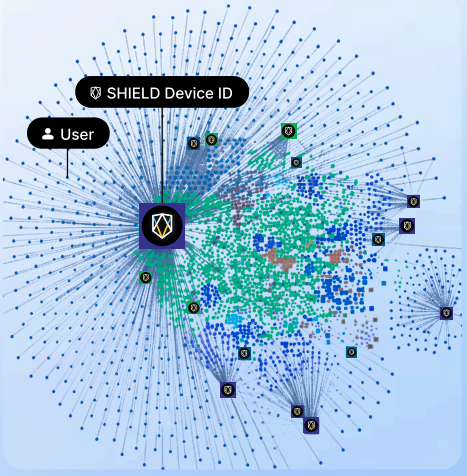
Dedy Giharto
Head of Technology, Treasury

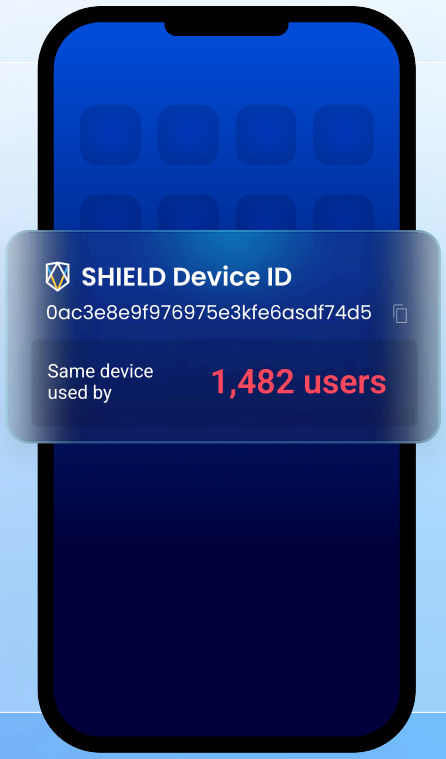
Our Solution

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

Prevent Market Manipulation Schemes

Understanding Market Manipulation

Market manipulation is the practice of artificially inflating or deflating the price of a stock or cryptocurrency. Fraudsters employ various tactics to achieve this including creating thousands of **fake accounts** to coordinate buying and trading activity, creating a false impression of high demand or scarcity.

Stop Pump & Dump Schemes

Prevent fraudsters from artificially inflating interest and prices with fake accounts. Leverage SHIELD's persistent device IDs to eliminate fake accounts at the root.

Block Wash Trading

Don't let fraudsters manipulate trading volume and liquidity. Stop trading controlled on the same device. Unmask tools used to aid malicious activity like app cloners & emulators.

Protect Crypto Communities

Safeguard your users from fake reviews and content. Prevent fraudsters from manipulating user perception, and competitors from leaving negative reviews.

SHIELD Fraud Intelligence

App Cloners Running
Emulator Running
VPN Running
Suspicious Factory Reset
Screen-sharing
Jailbroken Devices
Tampered apps

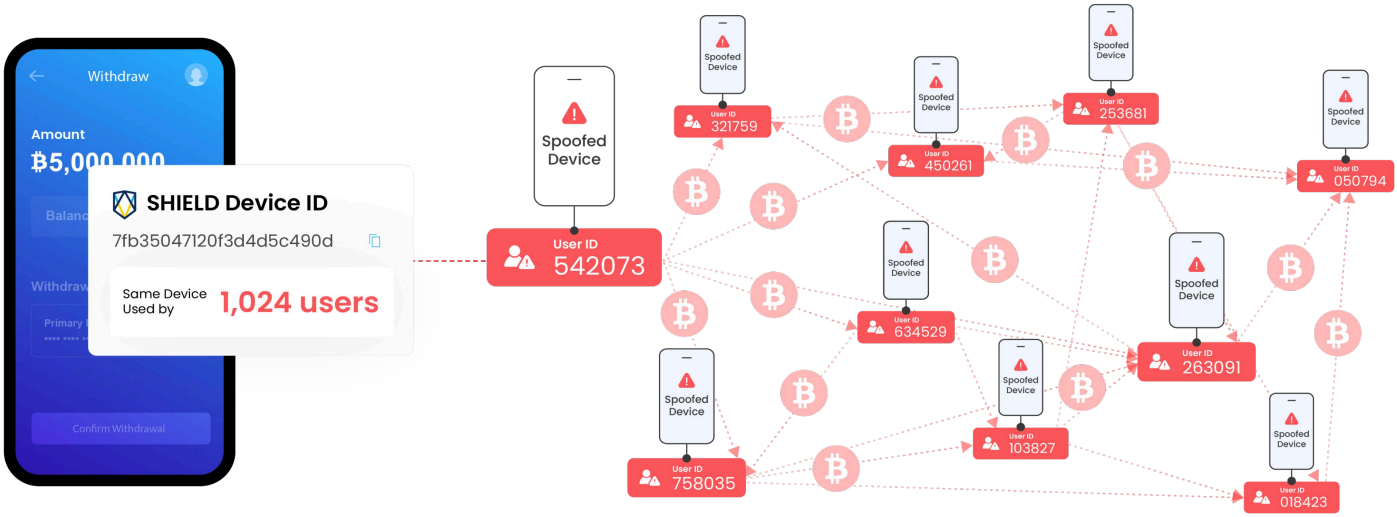
How it Works

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

Typically, fraudsters use fake accounts to conduct:

- Repeated trades in a short time frame, on accounts controlled by a single device
- Trades executed amongst multiple fake accounts, creating an illusion of high trading volume of liquidity - tricking users into investing into a shitcoin
- Coordinated buying and selling across a short duration from different locations
- Activities coming from devices in sanctioned locations

SHIELD identifies interconnected accounts controlled by the same device, revealing complex fraud clusters and stopping sophisticated coordinated attacks.



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

End Referral & Promo Abuse

What is Referral & Promo 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 results in lost revenue, and also skews marketing analytics on the success of promotional and referral campaigns.

SHIELD Fraud Intelligence

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

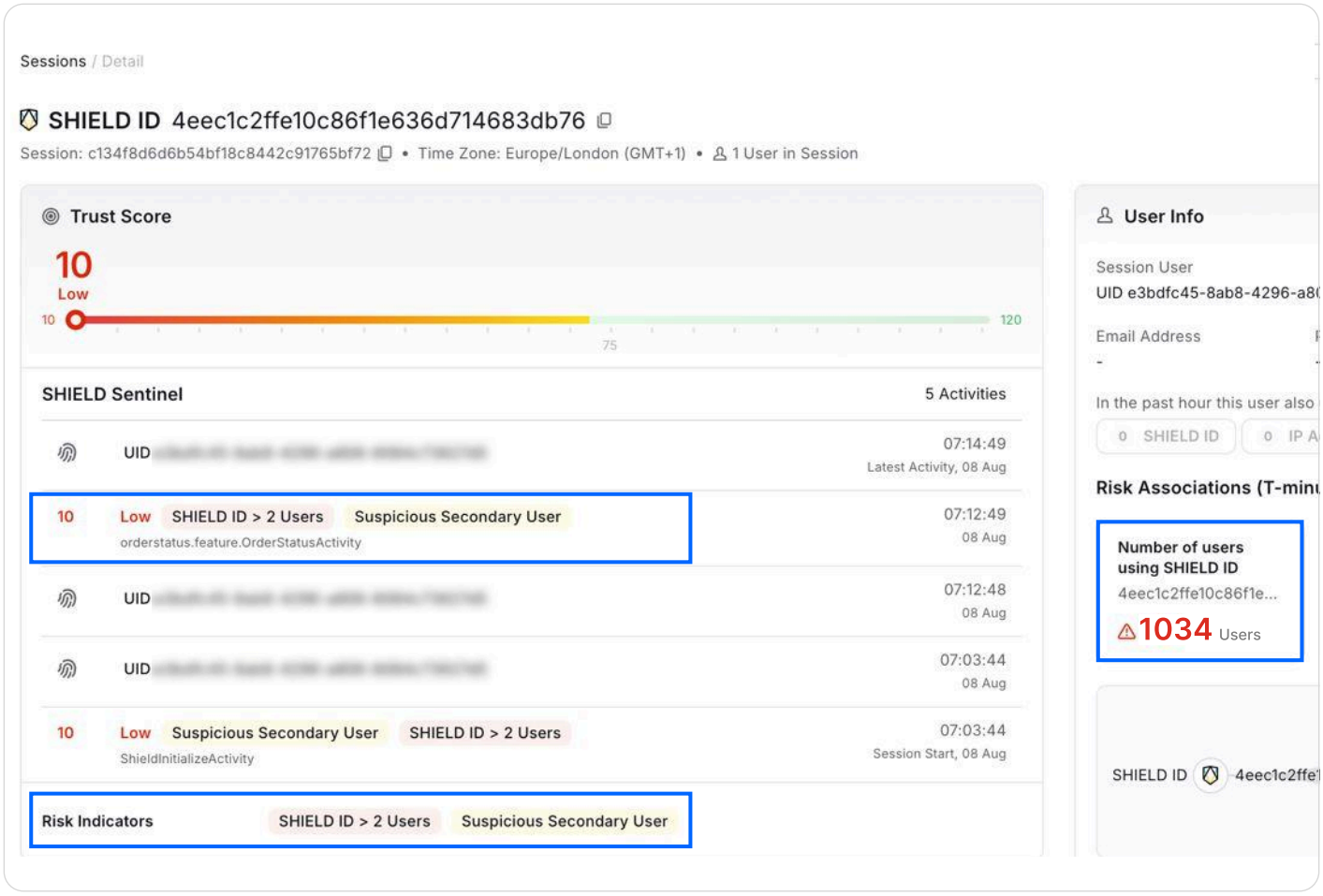
How it Works

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

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

Use Cases

Stop Location Spoofing & Money Laundering

What is Location Spoofing?

AML regulations often restrict trades from high-risk areas. Criminals can use location spoofing to bypass these sanctions. Banks that unknowingly process transactions originating from sanctioned locations risk violating AML regulations and facing penalties.

Identify High-Risk Logins and Transactions

Significantly reduce false positives with real-time risk monitoring that identifies fraudsters instantly. Leverage **trusted location** to stop transactions and logins from unauthorised locations, and users on PEP or sanction lists.

Provide Frictionless User Experiences

SHIELD combines **trusted location** intelligence with persistent device insights to identify trusted users. This reduces the need for additional verification steps like 2FA steps - only required when suspicious device behaviour is detected.