SHIELD

SHIELD for Banking Platforms

SHIELD's Device-First Fraud Intelligence platform identifies the root of fraud with the **SHIELD Device ID** and actionable **Fraud Intelligence**, helping banking platforms stay ahead of sophisticated complex fraud threats with high-performance algorithms.

Trusted by

truemoney maya :ubank FE CREDIT WINK ZIGI ... 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

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

SHIELD Fraud Intelligence
real-time actionable insights into fraudulent activity

Feature AI Engine
customize complex rules & policies to combat advanced attacks

Use Cases

Eliminate Money Laundering & Money Mules

What is Money Laundering and Money Mules?

Fraudsters use tools like app cloners and emulators to create fake account at high speed and scale. These accounts can act as vessels for money laundering, allowing money mules to deposit and transfer illegal funds. The ease and low cost of creating fake accounts makes it a challenge for banks to identify and eliminate them all.

01

Stop Fake Accounts & Money Mules at the Root

Eliminate fake accounts with SHIELD's persistent device IDs, built to withstand factory resets and advanced tampering.

02

Block Suspicious Activities in Real-Time

Stop mass account created on the same device. Unmask tools and techniques like app cloners & tampered apps used to aid suspicious activity.

03

Supercharge Mule Account Detection with Risk AI Models

2x your mule detection accuracy and enhance existing data models with SHIELD's actionable fraud intelligence and insights.

SHIELD Fraud Intelligence

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

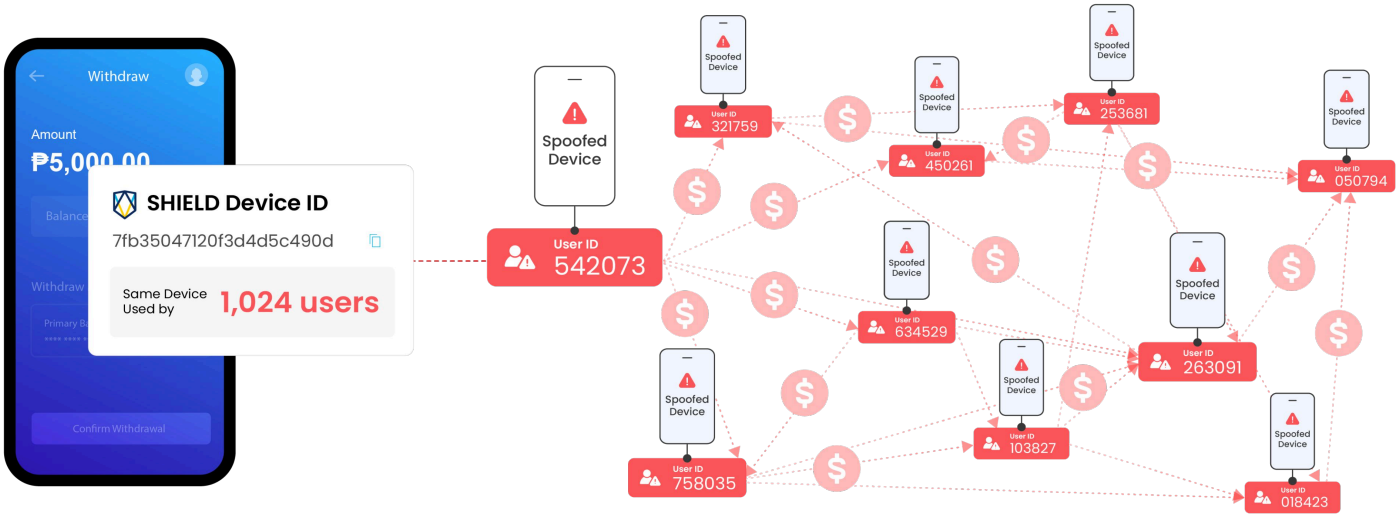
How it Works

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

Typically, fraudsters use fake accounts to conduct:

- Repeated small sum transactions in a small time frame to mule accounts
- Transactions executed by the same account, controlled by different devices across multiple locations
- Sudden withdrawals in a short duration from different locations
- Activities 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.

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 a bank executive to extract user credentials and details, taking over accounts and stealing funds. This leads to financial and reputational loss for banks.

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

Protect Against Payment Fraud

What is Payment Fraud?

Fraudsters can make unauthorized transactions with stolen card details and identities, which could result in high chargeback rates, financial losses, and loss of user trust and confidence.

Supercharge Transaction Monitoring with SHIELD's Feature AI Engine

Banking Ready Feature Sets

Leverage pre-built feature packages tailored to combat banking fraud.

Simplify feature creation, save time and effort, and stay in compliance with regulatory requirements.

Deployable at Every Checkpoint

Integrate seamlessly across the user journey, from onboarding and login to transactions.

Apply Feature AI where risk matters most, ensuring consistent protection without added friction.

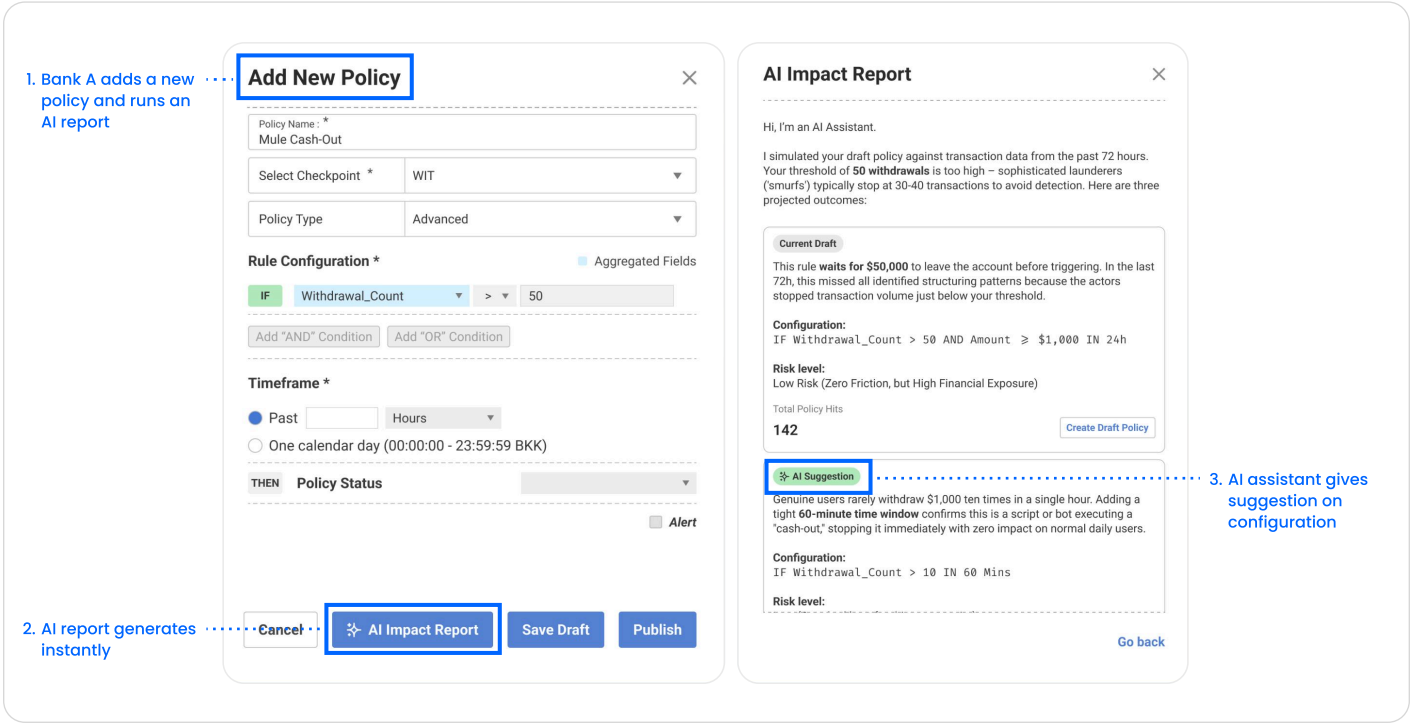
Enhanced by Device Intelligence

Unlock precise syndicate detection without disrupting user experience.

Link users, devices, and activities to identify coordinated attacks at the root.

Customize Risk Rules & Policies

Set customized and advanced policies across multiple checkpoints to meet complex financial and regulatory requirements. Run automated simulations to analyze how new policies affect your ecosystem before they go live.



Use Cases

Prevent Deepfakes & E-KYC Bypass

How Does E-KYC Bypass Happen?

Fraudsters bypass identity verification by injecting AI-generated deepfakes with **hooking techniques**, faking face, documents, and liveness checks. These attacks are often **carried out from the same device**, enhanced by app cloners and emulators. At scale, fraudsters automate attacks to mimic thousands of real users.

Curb Deepfakes & AI Fraud

Prevent fraudsters from using AI-generated deepfake videos and images to bypass biometric verification and trick liveliness detection.

Stop Hooking & App Tampering

Detect and block attackers who manipulate and tamper apps to disable app security measures and inject fake identity data.

Prevent Device Spoofing

Stop fraudsters from spoofing multiple device profiles and masking their real device identity with emulators, app cloners, and more.

The Fraud Landscape: Insurance & Lending

Across insurance and lending, bad actors are exploiting onboarding gaps, gaming instant approvals, and weaponising AI-generated documents.

Insurance Fraud & Policy Abuse

Identify Inflated Claims
Fraudulent or inflated claims slip through, enabling bad actors to extract payouts before detection kicks in.

Monitor Rogue Agents
Rogue agents and brokers create phantom policies or manipulate applications to hit quotas and earn commissions.

Stop Onboarding Fraud
Spot fake or duplicate applications and eKYC bypass attempts, stopping fraudulent policies before they're issued.

Loan Fraud & Identity Manipulation

Protect Against ATOs
Compromised accounts / Account Takeovers are used to access credit lines and withdraw funds, often before systems detect the breach.

Prevent Loan Stacking
Fraudsters exploit instant approvals to take out multiple loans across platforms, maximizing payouts before risk signals catch up.

Detect Synthetic Documents
AI-generated and cloned documents are used to bypass verification, enabling fraudsters to secure loans with synthetic or stolen identities.

Why SHIELD

The Limitations of Static App Hardening

Why isn't app hardening sufficient?

App hardening protects application code from tampering and reverse engineering, through code obfuscation and integrity checks. However, these protections are **static** and leave **critical detection gaps** during live user sessions.

As fraud tactics become more **sophisticated and AI-driven** (such as **deepfakes** and **automated attacks**), this lack of run-time insight **creates blind spots** that advanced fraud tools can exploit.

Detect Next-Generation Fraud Tools in Real Time

Modern fraud frameworks, such as AI-driven tools, are able to bypass static hardening protections by masking their traces.

SHIELD acts as an essential layer of defense, detecting these sophisticated fraud tactics at the very moment they are activated.

Protection Throughout the Entire User Session

Unlike app hardening, which focuses on code integrity, SHIELD provides **continuous, run-time visibility** into device behavior.

By monitoring device-level signals throughout the session, banks protect the entire user journey, from app launch, to login, to transaction.