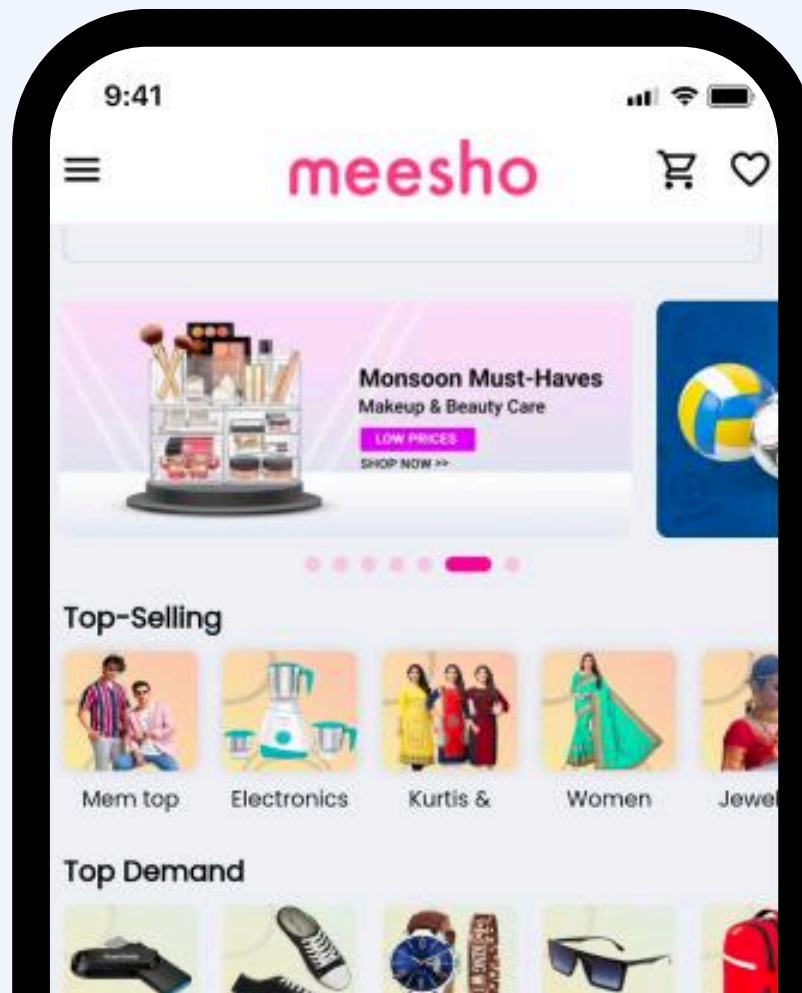


# How SHIELD helps Meesho stop fraud with its Device-First Fraud Intelligence Platform

Meesho is an Indian social commerce platform, with over 120 million monthly active users. It facilitates trade between suppliers, resellers, and customers. The platform provides a convenient way for individuals to enter the e-commerce space.

SHIELD's Device-First Fraud Intelligence platform consists of device identification and intelligence. We identify the root of fraud with the **SHIELD Device ID** and return **actionable fraud intelligence** in real-time, helping Meesho eliminate fraud.

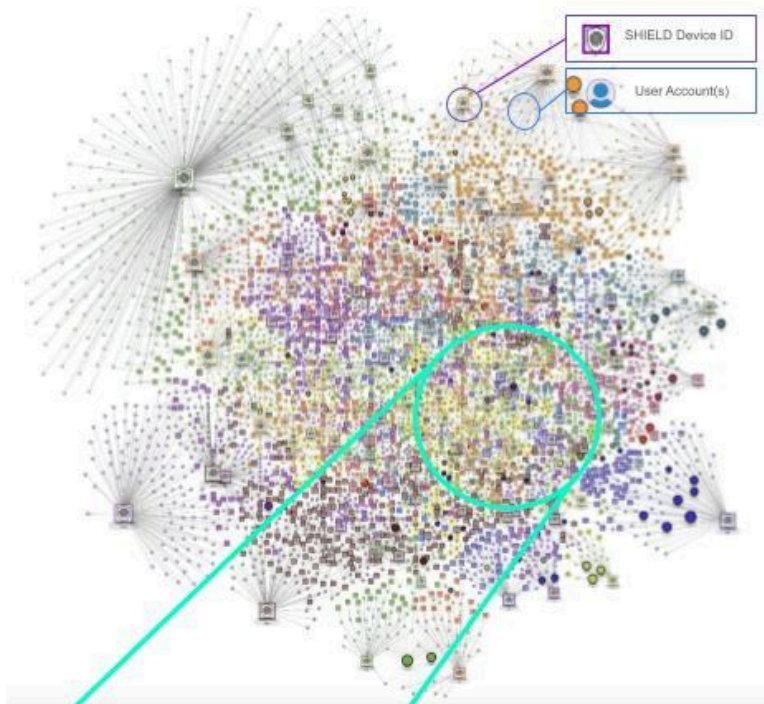




## Internal & Delivery Partner Fraud

### What is Internal & Delivery Partner Fraud?

Fraudulent delivery partners could collude to steal packages and goods from users and resell them, replacing the goods with defects or rubbish. This allows them to earn delivery fees, without delivering the actual goods.



### SHIELD Fraud Intelligence

App Cloners Running  
VPN Running  
Suspicious Factory Reset  
Hooking  
Screen-sharing

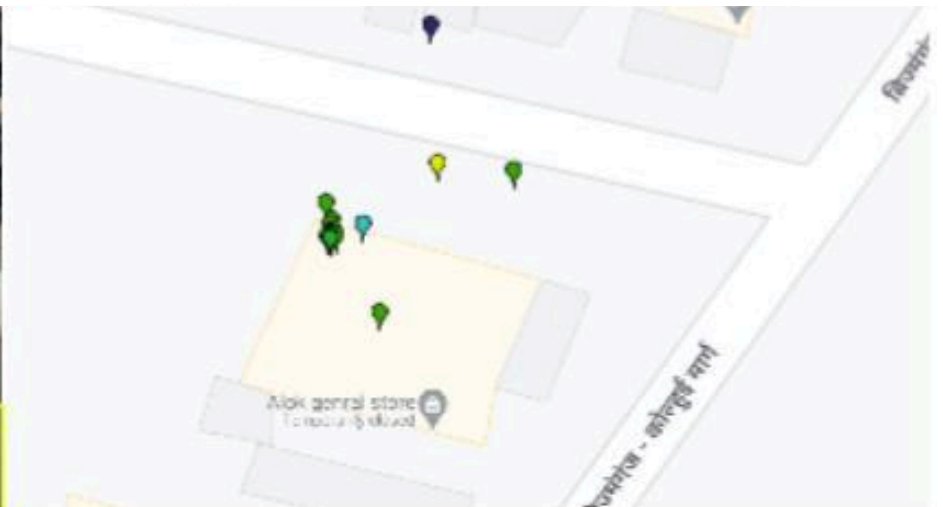
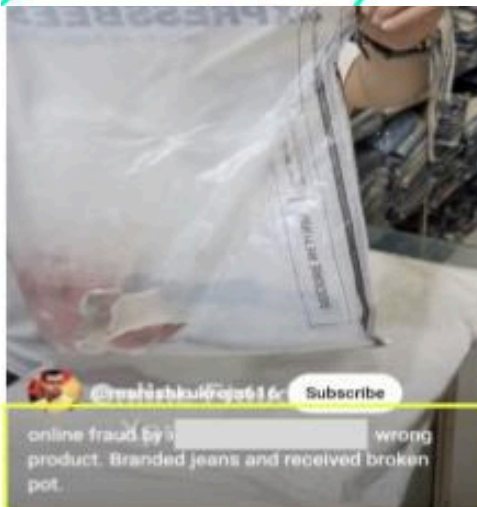
### Example Fraud Case:

**2,929 Devices** controlled  
**4,094 user accounts.**

Typically, **app-cloners** are used to create fake accounts at scale.

Fake accounts are often used to leave **fake ratings and reviews** that **enhance a listing's ranking** and **mislead genuine users.**

In one instance:  
SHIELD identified **15 devices** controlling **87 user accounts** connected to a client's logistics partners wifi network. Their location points to a logistics partner **warehouse.**





## Buyer-Seller Collusion

### What is Buyer-Seller Collusion?

Fraudsters create both buyer and seller accounts. They use **fake listings** to trick genuine users into purchasing counterfeit or defective products, using fake user accounts to bump up their listings with **fake reviews**.

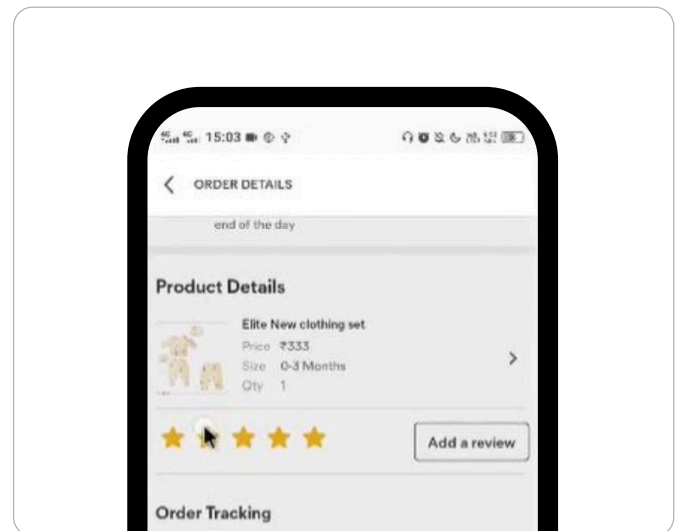
User can also earn rebates on marketplace apps. Fraudsters can work with seller to abuse this by buying an item and claiming rewards. The seller works with them to transfer back the value of the item so that no money has been spent, but reward points have been obtained. The user and merchant then tend to split the rebates.

## Fake Reviews

### What are Fake Reviews?

Fraudsters often create fake accounts to fake ratings at scale and boost the visibility of their fake listings.

- SHIELD Device ID identifies devices that are linked to multiple user accounts.
- SHIELD Fraud Intelligence detects commonly used tools and techniques to speed up the fake review creation process such as **app cloners and auto clickers**.



## Fake & Counterfeit Listings

### What are Fake Reviews?

Fraudsters create fake accounts to masquerade as legitimate brand affiliates and sell counterfeit or bad products.

- SHIELD Device ID identifies devices that are linked to multiple user accounts.
- SHIELD Fraud Intelligence detects commonly used tools and techniques used to create fake listings at scale such as **app cloners and emulators**.





## Referral & Promo Abuse

### What is Referral & Promo Abuse?

Fraudsters can create many fake accounts to redeem the same discounts multiple times, draining campaign budgets. They could also exploit new-user signup and referral codes in the same way. SHIELD **identifies devices linked to multiple user accounts**, and detects tools used by fraudsters to automate and scale this process.

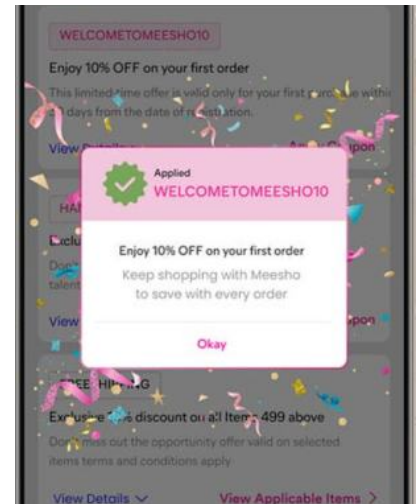
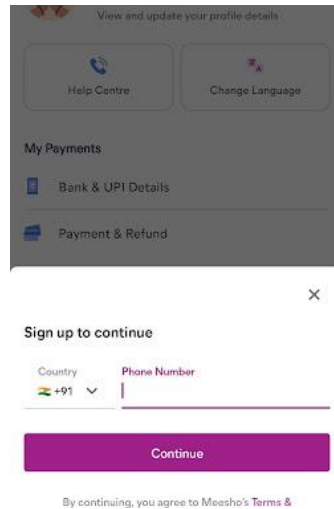


#### SHIELD Fraud Intelligence

Detects commonly used tools and techniques to speed up the promo redemption process such as **app cloners and tampered apps**.

These malicious tools are used to change device attributes.

This allows fraudsters to evade detection and create multiple accounts at scale, abusing sign up bonuses for new users, referral codes, and limited time discounts.



**SHIELD Device ID**  
2e1c3e3bb22625f9e8cfd718f1b28062

Device used by **1055** users (Last 30 days)

Platform

**Session History** 27 Jun - 28 Jun

All 68 users

Time	Risk	Session ID
14:27	10 High	c76e9a5a...5e9e26be
14:27	10 High	dac82968...b7094220
14:23	10 High	c89d478d...2cf28a96
14:20	10 High	b597e253...7fe06cad

**10 High** Session ID c76e9a5a527c47cabebf8c225e9e26be | 28 Jun 2024.

**Device**

**Risk Score** 10 High

**Fraud Intelligence**

- App Cloner Running
- App Tampering

**SHIELD Sentinel**

14:27 High 10

- App Cloner Running
- App Tampering

activities AccountContainerActivity



## Account Takeover (Abusing Accessibility Services)

### What is Referral & Promo Abuse?

Fraudsters can create many fake accounts to redeem the same discounts multiple times, draining campaign budgets. They could also exploit new-user signup and referral codes in the same way. SHIELD **identifies devices linked to multiple user accounts**, and detects tools used by fraudsters to automate and scale this process.

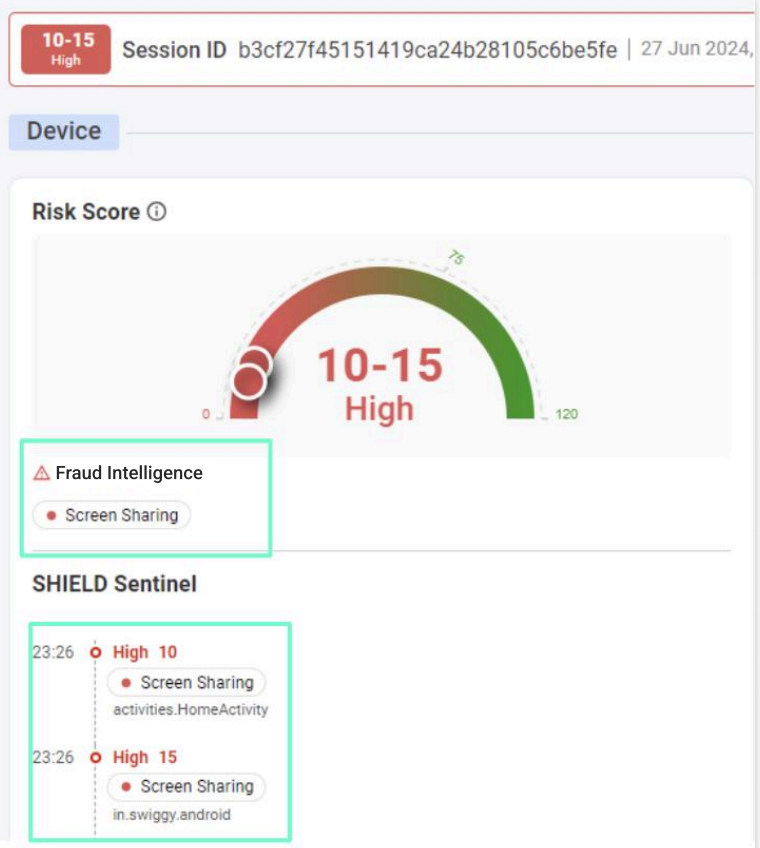
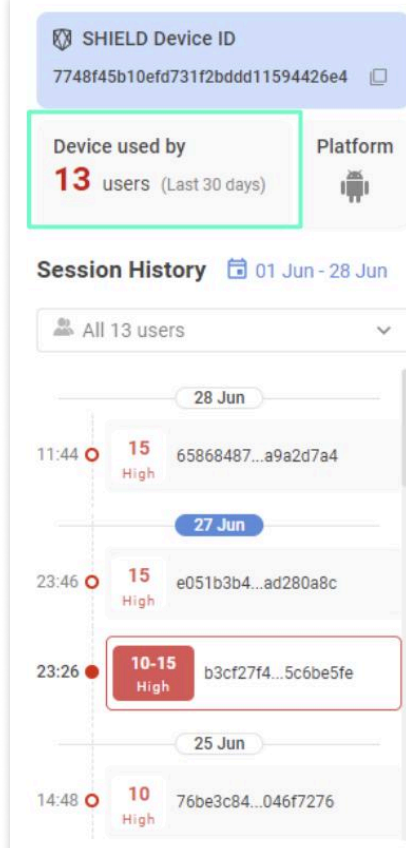
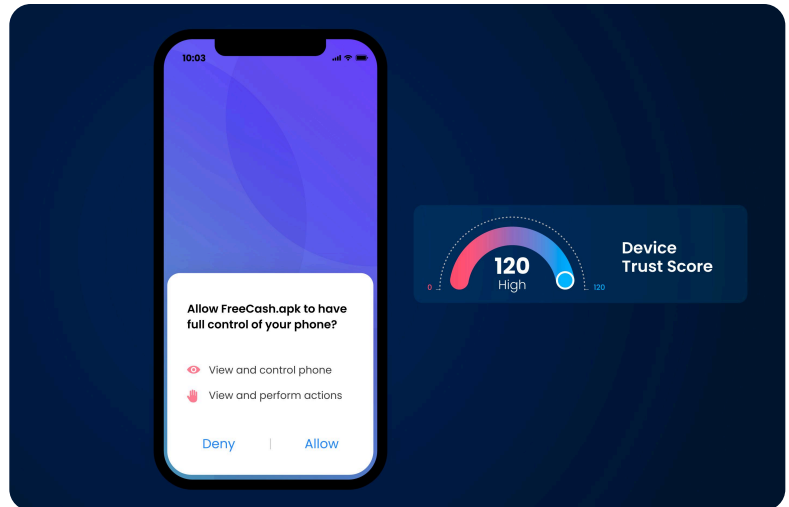


### SHIELD Fraud Intelligence

SHIELD's Fraud Intelligence continuously profiles device sessions, **returning when a good user turns bad**.

For example, SHIELD can detect when devices with a consistently high trust score suddenly begin to exhibit malicious behaviour, returning risk signals including:

- The use of **screen-sharing tools, auto-clickers, and device masking tools** - often used by ATO fraudsters.





# Account Takeover

## What is Account Takeover?

Account takeover (ATO) fraud is when fraudsters gain unauthorised access to user accounts with stolen credentials. They use credential stuffing and brute force attacks to conduct mass takeovers. Once in, fraudsters are able to do a myriad of fraudulent activities, including **payment fraud** and stealing personal information.

### 01

#### Payment Fraud

Fraudsters with access to user accounts can steal user information, including credit card details, using the victim's information to make unauthorized transactions.

### 02

#### Refund Fraud

Fraudsters change user card information or bank details to their own without the victim's knowledge, claiming any refunds made.



#### SHIELD Fraud Intelligence

Detects when multiple accounts are being accessed by one devices - a sign that a fraudster is attempting to takeover accounts.

Multiple login attempts in a short period of time, across multiple geographical locations are also flagged as suspicious activity.

SHIELD also detects commonly used tools and techniques to speed up the ATO process such as emulators and jailbroken devices.

The screenshot displays the SHIELD Fraud Intelligence interface. On the left, a 'Session History' table lists sessions for 27 Jun - 28 Jun, with a filter for 'All 5 users'. The table shows a series of sessions on 28 Jun, each with a 'High' risk score and a unique SHIELD Device ID. On the right, a 'Device' overview card shows a 'Risk Score' of 10 (High) on a gauge. Below this, 'Risk Indicators' are listed: Emulator, Jailbroken/Rooted, App Tampering, and Debugging. The 'SHIELD Sentinel' section shows a specific session at 16:48 with a 'High 10' risk score and the same indicators. At the bottom, a 'Device Fingerprint' section lists: SHIELD ID (c4d49905c4e1371b0445b8230e49fcb4), Device Brand (google), Device Model (sdk\_gphone\_arm64), and Battery Level (100%).

Time	Risk	Device ID
12:09	High	37a0d479...eef37ecc
12:06	High	6ee83aae...f65bb50f
12:04	High	b02267c0...e02a3234
12:00	High	7db97941...1c7d9a2d
11:44	High	458722d7...da07158f
11:42	High	4f0c60fd...7376fce8
11:38	High	eb2e2d76...38277fb3
11:38	High	cabd36fd...d811726d