



# SHIELD para E-Wallets & Superapps

A plataforma de inteligência de fraude focada na identificação de dispositivos da SHIELD identifica a raiz da fraude por meio do **SHIELD Device ID** e do **Fraud Intelligence**, ajudando e-wallets a proteger informações dos usuários e se anteciparem a ameaças sofisticadas de fraude.

Quem Confia em Nós

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

“O parceiro perfeito para nós precisa ser capaz de escalar junto com a TrueMoney, possuir forte expertise técnica em e-wallets e a agilidade para se manter à frente dos comportamentos em constante mudança tanto dos fraudadores quanto dos consumidores. A SHIELD preenche todos esses requisitos.”



**Monsinee Nakapanant**  
Co-Presidente, Ascend Money

## Nossa solução

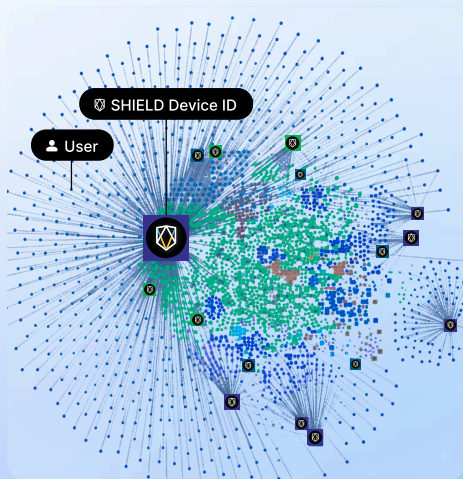
Plug-and-Play

Sem códigos adicionais

Não requer PII

### SHIELD Device ID

identifica de forma persistente a raiz da fraude & contas falsas >99.9% de precisão



### SHIELD Device ID

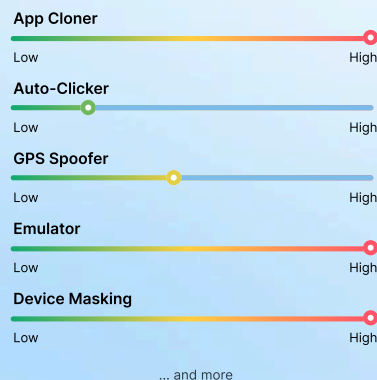
0ac3e8e9f976975e3kfe6asdf74d5

Same device used by **1,482 users**

### SHIELD Fraud Intelligence

insights acionáveis em tempo real sobre atividades fraudulentas

#### 20+ Sinais de Risco Configuráveis





## Elimine Abuso de Promoção & Incentivos

### O que é abuso de promoção & incentivos?

Fraudadores podem criar múltiplas contas falsas para explorar promoções de cadastro de novos usuários e programas de indicação. Para criar essas contas falsas, utilizam identidades roubadas e documentos falsificados para burlar verificações de KYC. Isso gera números de crescimento inflados, perda de receita e confiança, além de distorcer métricas de marketing relacionadas ao desempenho das campanhas.



### Exploração de Promoções para Novos Usuários

Impeça fraudadores de abusarem de promoções voltadas para novos usuários por meio de contas falsas criadas para resgatar recompensas, como cashback, repetidamente.



### Conluio & Abuso de Programas de Cashback

Bloqueie esquemas em que usuários e lojistas se unem para simular compras falsas. Nessas fraudes, usuários pagam com pontos, recebem cashback e dividem os ganhos com os lojistas, enquanto os lojistas reembolsam os usuários e evitam taxas.



### SHIELD Fraud Intelligence

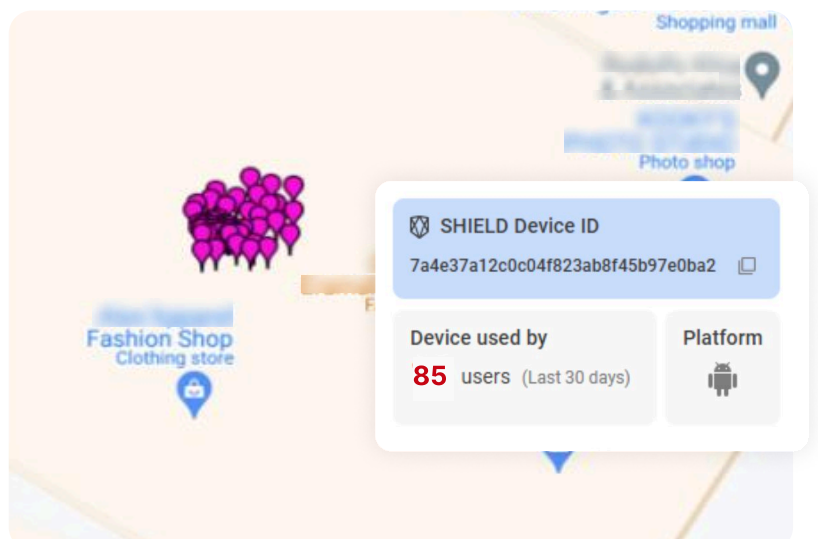
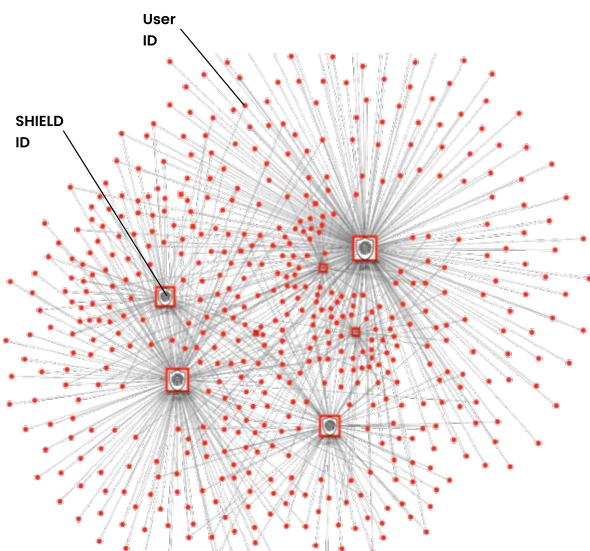
Uso de App Cloner  
Uso de Emulador  
Reset de Fábrica suspeito  
Jailbroken Devices  
Tampered apps  
Auto-clickers

### Como Funciona

Fraudadores criam contas falsas em escala utilizando identidades roubadas, apps adulterados e emuladores. Essas contas são usadas para:

- Aproveitar bônus de cadastro para novos usuários
- Explorar programas de indicação ao indicar contas controladas pelo próprio fraudador
- Realizar conluio com lojistas para concluir transações fraudulentas

A SHIELD identifica persistentemente dispositivos vinculados a múltiplas contas por meio do SHIELD Device ID. A inteligência acionável de fraude da SHIELD revela ferramentas utilizadas na criação de contas falsas, como clonadores de aplicativos e emuladores. Combinada à inteligência de localização, a SHIELD ajuda a identificar hotspots de fraude e revelar a real dimensão das atividades fraudulentas.



# Elimine Fraudes de Account Takeover

## Abuso de Serviços de Acessibilidade & Engenharia Social

### O que é Fraude de Account Takeover?

A fraude de account takeover (ATO) ocorre quando um fraudador obtém acesso às credenciais de login da vítima para roubar fundos ou informações.

**01**

### Abuso de Serviços de Acessibilidade

As vítimas, sem saber, baixam e concedem permissões de acessibilidade a aplicativos maliciosos. Isso permite que os fraudadores ganhem controle sobre o dispositivo, roubando dados, OTPs e mais.

**02**

### Engenharia Social

Fraudadores se passam por ou fingem ser um executivo bancário para extrair credenciais e detalhes dos usuários, assumindo o controle das contas e roubando fundos. Isso leva a prejuízos financeiros e de reputação para os bancos.





## Elimine Contas Falsas & Mulas de Dinheiro

### O que são Contas Falsas e Mulas de Dinheiro?

Fraudadores usam ferramentas, como clonadores de aplicativos e emuladores, para criar contas falsas com alta velocidade e escala. Essas contas podem servir como veículos para lavagem de dinheiro, permitindo que "mulas" de dinheiro depositem e transfiram fundos ilegais. A facilidade e o baixo custo de criar contas falsas tornam um desafio para os bancos identificar todas e eliminá-las.



#### Forneça uma Experiência do Usuário sem Fricção

A SHIELD combina inteligência de localização com insights persistentes de dispositivos para identificar usuários legítimos. Reduza custos com OTP e minimize a necessidade de autenticação em dois fatores, acionadas apenas quando comportamentos suspeitos forem detectados no dispositivo.



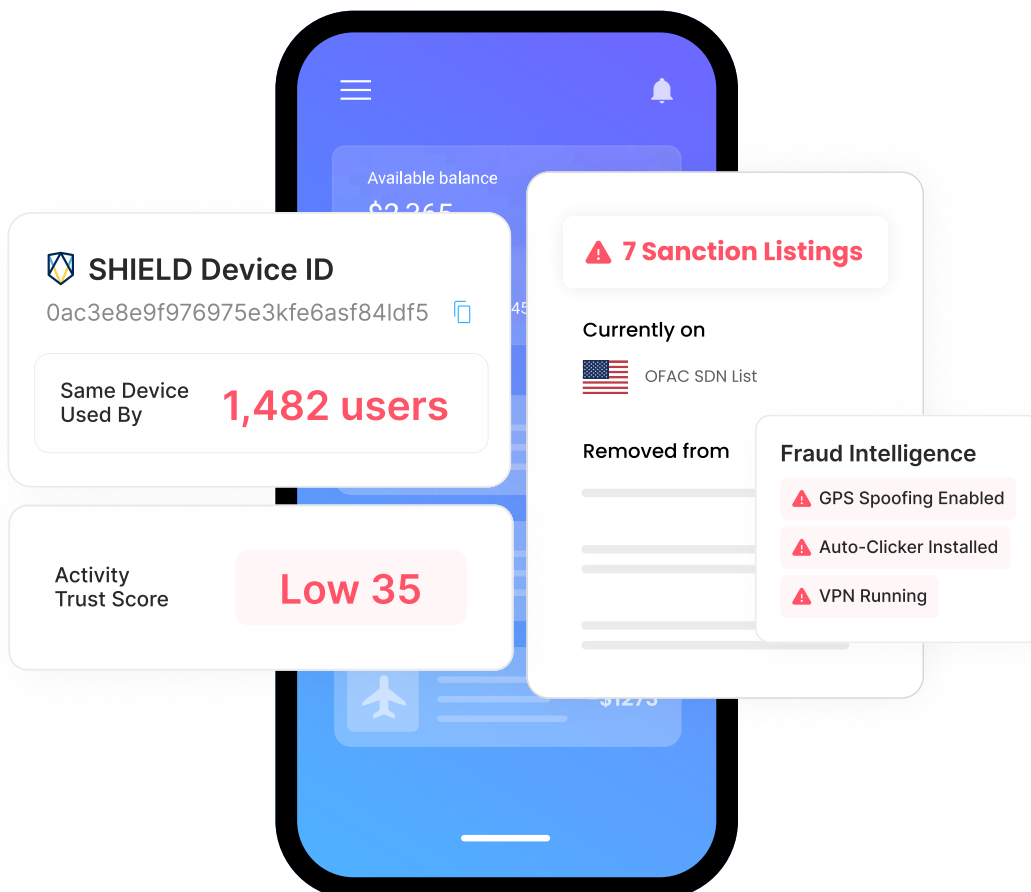
#### Identifique Atividades de Alto Risco

Reduza significativamente falsos positivos com monitoramento de fraude em tempo real. Utilize inteligência de localização para bloquear atividades originadas de locais não autorizados e verificar listas de sanções. Tudo isso mantendo conformidade com requisitos regulatórios.



#### Potencialize a Detecção de Contas Mula

Duplique a precisão na detecção de contas mula e fortaleça modelos de dados existentes com inteligência acionável de fraude. Elimine contas falsas com os Device IDs persistentes da SHIELD, desenvolvidos para resistir a resets de fábrica e técnicas avançadas de adulteração.





A Vantagem da SHIELD

# Prevenção de Fraude que se Paga

## À Prova de Falhas

### >99.99% de Precisão

Resistente a qualquer tipo de adulteração (resets de fábrica, clonagem, etc)

### Agnóstica a Indústria e Região

Funciona em qualquer lugar, para qualquer indústria.

### Construída para todos os casos de uso

Cobre os principais desafios de fraude sem comprometer a experiência do usuário.

## Time-to-Value Rápido

### Plug & Play

Integração simples, com esforço mínimo de engenharia.

### Sem período de treinamento

Curva de aprendizado zero, com insights imediatos desde o primeiro dia.

### Sem Necessidade de PII

Evite barreiras de compliance. Funciona com as permissões já existentes no aplicativo.

## Flexível para Escalar

### Personalizável para as Necessidades do Negócio

Mais de 20 sinais de risco configuráveis.

### Total Propriedade dos Dados

100% dos dados enviados e retornados pertencem à sua empresa.

### Escala Junto com Você

A SHIELD se adapta às suas necessidades de risco em cada estágio de crescimento.

