IDMERIT™
VERIFY ANYONE, ANYTIME, ANYWHERE

Fraud Prevention Suite

Prevent Fraud Using Device Fingerprinting

Built-in safeguards for a smooth customer experience

App/website Opening → Login & Authentication → Transactions & interactions → Post transactions & periodic updation

- **Account Takeover Fraud**
  Combat unauthorized access and protect customer accounts
- **Social Engineering Fraud**
  To secure customers against phishing attacks.
- **Promotion abuse**
  To mitigate the risk of fraudulent use of offers
- **Identity fraud**
  To prevent credentials from being spoof by fraudsters

- **Account Mules**
  Mitigate the risk of unauthorized access to customer accounts.
- **Buyer-seller-agent collusion fraud**
  Identifying and preventing fraud rings and collusion networks
- **Chargeback Fraud**
  To defend their customers against phishing attacks
- **Fake refund claim**
  To Prevent credentials from being spoof by fraudsters

IDMERIT Fraud Prevention Suite

IDMERIT helps businesses fight fraud by using unique device signals to identify suspicious activity throughout a user's journey. Using two different components, we are able to provide frictionless fraud fighting capability passively through our solution

Device Intelligence

The device-level data can be used to assess the user's authenticity beyond their document proofs.

Device Fingerprint

A unique device identifier can be built by detecting hardware and software characteristics of a device

Device-level Signals

The device-level data can be used to determine a user's genuineness beyond his or her document proofs, for example, VPN, proxy, emulator, bot, remote viewer, spoofing, rooted device checks, trueOS, true IP addresses.

Risk Signals

Device related

- App tampering
- App cloning
- Emulator
- Debuggable
- Rooted
- Mock GPS
- Remote session
- Voice call
- Developer Mode
- Accessibility Mode
- ADB Enabled
- Play Store / App Store Install

IP Security

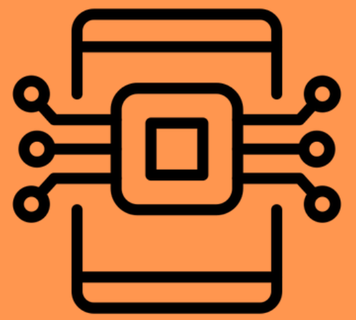
- Proxy
- VPN
- Tor
- Crawler
- IP Address

Fingerprint related

- First seen date
- User ID Count

Network related

- ISP Name
- IP type - home /commercial



Browser-level Signals

Analyze the user's browser-level data to detect any anomalies, such as the use of a VPN, proxy servers, or incognito/private browsing mode. This information can help determine if the user's identity matches their claimed identity.

Risk Signals

Browser related

- Incognito
- Ad Blocker
- Anonymisation attempted
- True user agent
- Timezone manipulation

Network related

- ISP Name
- IP type - home / commercial

IP Security

- Proxy
- VPN
- Tor
- Crawler
- True IP Address

Fingerprint related

- First seen date
- User ID Count

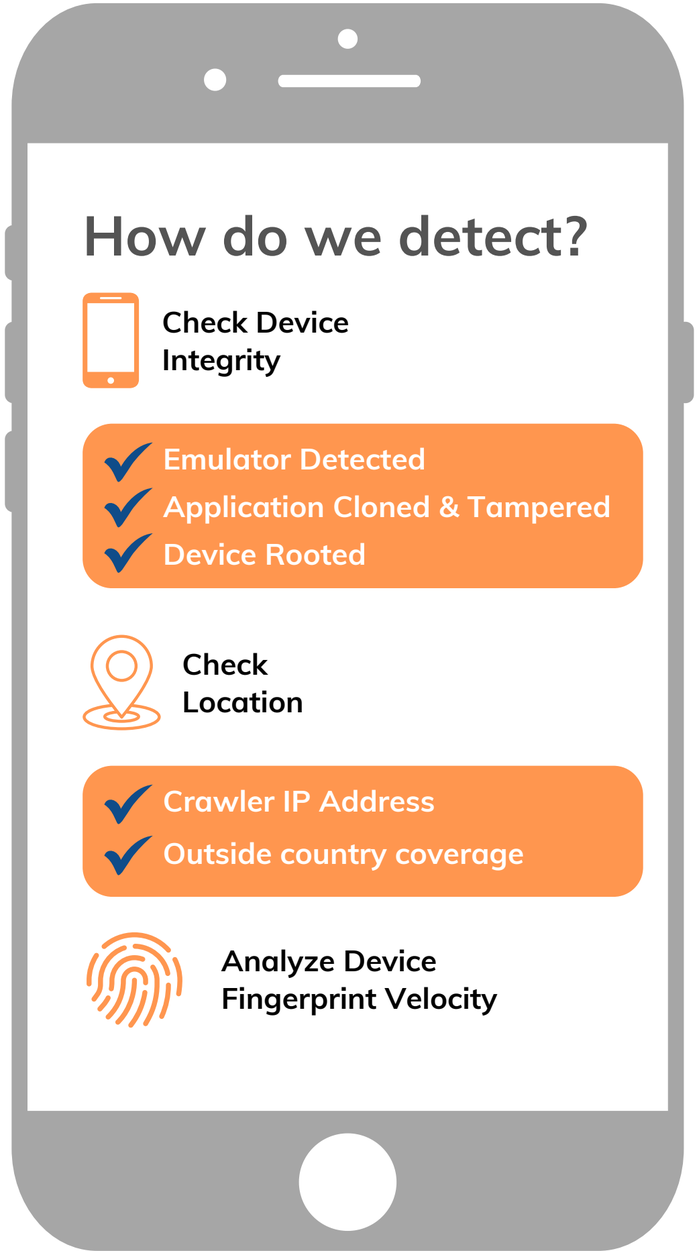
User Onboarding Protection

Fraud Problem:

- **Account Opening Fraud**
  Authentic customers have a seamless experience when opening an account.
- **Identity Fraud**
  Fraudulent account openings can be detected in real time.
- **Promotion/ Referral Abuse**
  Referral deals should be protected from abuse by users.

Fraud Pattern:

- **Account Opening Fraud**
  - User authentication attempt from a high-risk device.
  - Multiple accounts are created by user on a single device.
- **Identity Fraud**
  - User was pressured into creating an account
  - Multiple accounts are created on the same device by the same user
- **Promotion/ Referral Abuse**
  - Referral deals should be protected from abuse by users.
  - Multi-device & multi-account links detected



User Login & Authentication Protection

Fraud Problem:

- **Account Takeover Fraud**

  Protecting account of a customer from unauthorized access.

- **Social Engineering Fraud**

  Safeguarding customers against phishing attacks

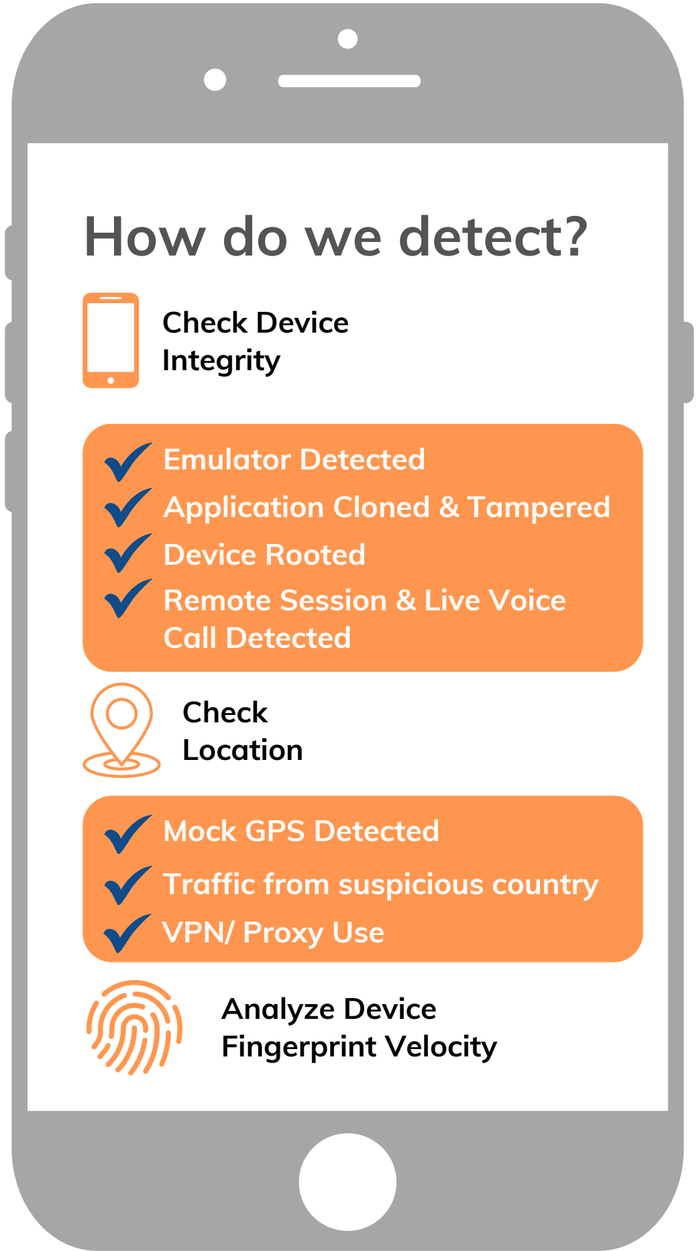
Fraud Pattern:

- **Account Takeover (ATO) Fraud**

  1. Uncertainty exists about device integrity
  2. Detection of Automated sessions
  3. Detection of Location anomalies
  4. Multiple login attempts in a short period of time

- **Social Engineering Fraud**

  1. Geopositional inconsistency and suspected location masking
  2. Detection of Live voice call and remote session
  3. Same IP address or device used by multiple users
  4. Detection of multiple location or new country



Transaction/ Payment Protection

Fraud Problem:

- **Online Payment Fraud**
  To protect the customer against unauthorised payments
- **Buyer-Seller Collusion Fraud**
  Safeguarding your platform against money laundering schemes and exploitation of promotional offers by colluding fraudsters.
- **Triangulation Fraud**
  To safeguard your platform from malicious users creating fake storefronts.

Fraud Pattern:

- **Online Payment Fraud**
  1. A threat to device integrity
  2. Location mismatch and concealment attempt detected
- **Buyer-Seller Collusion Fraud**
  1. Unusual change in IP/Network, new country
  2. Same device used for creating multiple user accounts
- **Triangulation Fraud**
  1. Multiple accounts are created on the same device by the same user
  2. Multi-device & multi-account links detected
  3. Automated session detected

Post-Payment Protection

Fraud Problem:

- **Chargeback Fraud**

  To distinguishing genuine dispute from fraudulent chargebacks

- **False Refund**

  Safeguarding your platform against money laundering schemes and exploitation of promotional offers by colluding fraudsters.

Fraud Pattern:

- **Online Payment Fraud**

  1. A threat to device integrity
  2. Location mismatch and concealment attempt detected

- **Buyer-Seller Collusion Fraud**

  1. Unusual change in IP/Network, new country
  2. Same device used for creating multiple user accounts

- **Triangulation Fraud**

  1. Multiple accounts are created on the same device by the same user
  2. Multi-device & multi-account links detected
  3. Automated session detected

IDMERIT™

Our Clients

Paysafe:

TransUnion

eToro

LSEG

SheerID

match

BrightSwipe

tribal

BANCO DINO

Trulioo

weThink

APOMEDICAL

KAJABI

rater

MANGATA PAY UK

tiller

Case Studies

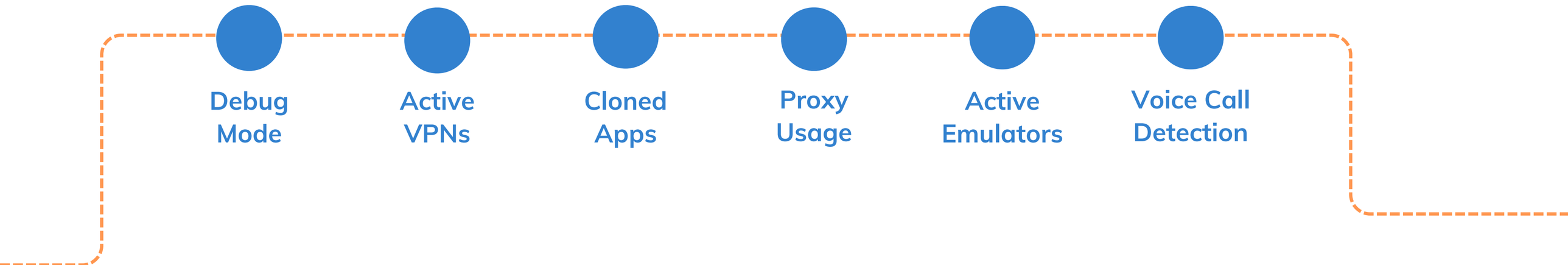
Gig Economy - Logistic Industry

Online Payment Fraud

Scammers impersonating genuine transportation companies ask for advance payments and disappear after the advance payment has been received.

Signal Analysis

High to medium risk signals identified:



How to use Device Intelligence Signals

A seamless user account opening and login experience can be delivered to **users with low-risk device signals**.

When a user opens a user account with **medium to high risk signals**, additional security measures such as additional verification steps can be enforced.

To prevent users from logging into their accounts when suspicious login patterns are detected, such as multiple accounts on the same device or an abnormal number of logging in sessions in a short period of time.

FinTech Industry - Lending & Wealth

Account Takeover Fraud

Login credentials are stolen or vulnerabilities are exploited by fraudsters to gain access to accounts. Unauthorized transactions are then initiated by them.

Chargeback Fraud

Fraudsters infiltrated accounts and applied for services without knowledge of account holders. Account holders then disputed the charges.

Signal Analysis

High to medium risk signals identified:

How to use Device Intelligence Signals

When suspicious login patterns, such as multiple accounts per device or an abnormal number of login sessions within a short period of time, are detected, users flagged with high-risk signals are barred from accessing their accounts.

In order to prevent high-velocity actions from being taken against devices with the same IP address, you can throttle or block them.

Online Gaming Industry

Collusion Fraud

A number of players are colluding to raise the odds of social betting in their favor.

Promotional Abuse

A number of fake accounts were used by fraudsters to take advantage of gaming incentive promotions.

Signal Analysis

High to medium risk signals identified:

- Active Emulators
- Cloned Apps
- Device Fingerprint Velocity

How to use Device Intelligence Signals

Using device intelligence, multiple synthetic accounts and SIM cards were found on the same device, as well as suspicious fingerprints on it

Why partner with IDMERIT?

- Easy and Simple Integration
- Low Operational Costs
- Enhanced User Experience
- AI Driven Comprehensive risk scoring
- Reduced Fraud Losses
- Easily configured for business

IDMERIT at a Glance

- **Global Presence**
- **90+** Enterprises
- **400M+** Verified ID's
- GDPR Compliant