Shufti

Transaction Trust Screening

AI-powered fraud prevention for faster, smarter transaction decisions.

PCI DSS · SOC2 · GDPR · QG GDPR · ISO 27001: 2013 · CE+ · iBeta Level 1 · iBeta Level 2 · KJM Verification age · CCPA

Online payments keep speeding up , and so do fraudsters. Traditional rule stacks struggle to keep pace, and teams drown in manual tuning. Shufti's answer is simple: our **Transaction Trust Screening** product delivers AI-powered fraud detection built directly into Shufti's ecosystem.

It operates through two touchpoints of our platform:

- **Back Office:** where your risk teams monitor, investigate, and tune strategy
- **Real-time APIs:** which screen every transaction before authorization to make a fast, explainable decision, before authorization costs accrue.

At its core is Shufti's globally trained AI engine. It evaluates device, network, identity, payment, and behavioral context in milliseconds , returning a transparent score, detailed explanation, signals, and a decision. As it continuously learns from live outcomes, you get enterprise-grade fraud defense without operational overhead.

Why This Works for Shufti Customers

- Real-time scoring with no ongoing model maintenance
- Decisions informed by global intelligence and live behavioral data
- Advanced controls through one Shufti API + Back Office
- Scales from thousands to millions of transactions across industries

Where It's Used & How It Flows (Merchant & PSP)

Merchant Use (Pre-Authorization Screening)

Start screening before you send traffic to the processor, so only trusted transactions reach the issuer.

End-to-end flow

- Customer initiates checkout on your site/app.
- Your system sends available data to Shufti (IP, device, amount, shipping, and, if PCI-compliant, card hints such as brand/BIN).
- Shufti responds in real time with Approve / Decline / Manual Review / Custom Action (e.g., step-up KYC or Strong Customer Authentication routing).
- You act on the decision and send a sync status update (e.g., approved, declined).
- If later outcomes emerge, send async updates (e.g., chargeback, fraud_confirmed, debt_collection_loss). This keeps the model current and adaptive.

Why Pre-Screening Matters?

Block fraud before fees and downstream costs

Keep processor traffic clean, improving authorization rates

Protect conversion by confidently approving good users

PSP / Payment Orchestrator Use

The PSP hosts checkout, forwards transaction + payment data to Shufti, then routes authorization.

Payment Service Provider Cycle

- PSP collects transaction and payment data (often on a hosted page).
- PSP forwards to Shufti and receives a decision.
- PSP proceeds or halts; sends sync updates post-authorization and async updates for late truths (e.g., chargebacks).

Even though PSPs and merchants use different identifiers (Client ID for PSPs, Seller ID for merchants), Shufti's learning and improvement process remains consistent across all transactions.

What You Receive Per Transaction

Score (1–100)
Higher = higher fraud likelihood; tuned to global and client-specific traffic patterns.

Story (Why)
Human-readable rationale: e.g., geo mismatch, device reputation, velocity anomalies.

Signals
Hundreds of evaluated attributes across five categories , geo, user, transaction, funding_source, seller.

- **Red** = risky (e.g., proxy IP, mismatched addresses)
- **Green** = trustworthy (e.g., consistent identity/payment)
- **Gray** = neutral/insufficient data

Decision
Approve, Decline, Manual Review, or Custom Action (step-up KYC/OTP/SCA routing, hold-for-review, webhook to fraud ops). A Watch mode is available to observe behavior without enforcement.

Related Transactions
Links activity across ~12 months on key identifiers like email, customer name, ID, payment, phone, device ID, IP, and shipping address.

Shufti's AI engine evaluates each transaction based on five pillars:

- **Geolocation:** IP and geo patterns
- **Payment:** Amount, currency, method/brand
- **Customer:** Name, email and behavioral traits
- **Transaction:** Pattern comparison across merchants and channels
- **Merchant:** Behavioral baselines for the same merchant

Data Depth & Enrichment (Turning Raw Data into Signal)

Shufti's AI engine processes and enriches payment and contextual data into high-signal attributes that drive accurate decisions.

Examples Of Enrichment

Email

- Domain risk
- Age
- Breach association

IP/Network

- VPN/TOR/hosting
- Bot/recent abuse
- ISP class
- Geo accuracy

Device

- Fingerprint (via optional script)
- OS
- Timezone
- persistent device_id
- Plugins
- language

Cards/Payments

- BIN country/brand/sub-brand
- CVC results
- Expiry windows

Industry lenses

- Airlines (legs, timings)
- Gaming (platform, rank)
- Hotels (length of stay)
- BNPL (missed payments)

Industry-Specific Data Points

Airlines

- airticket_days_to_departure
- airticket_airline_name
- airticket_departure_ts
- airticket_leg1_price

BNPL

- bnpl_credit_check_performed
- bnpl_missed_payment_count

Digital Goods

- digital_product_type
- digital_event_date

Bank Transfer

- ba_iban

Gaming

- gaming_user_ranking
- gaming_platform

Cards

- cc_num_hash
- bin_ctry

Hotels

- hotels_days_until_stay
- hotels_payment_type

General Payment

- pmt_method
- pmt_method_brand

In total, Shufti supports more than 500+ predefined data points that you can use to define and refine rule logic.

Rules You Control

Authoring, Priorities & Testing

Create, simulate, and instantly publish rules directly within the Shufti Back Office, no coding required.

Authoring flow

Step 1

Name + Description

Step 2

Choose Action

(Approve, Decline, Watch, Manual Review, PSD2 Exemption, Custom)

Step 3

Set Priority

(High, Low, Medium)

Step 4

Add Attributes With Operators

(Equals, Contains, Greater-Than, Etc.)

Step 5

Submit

Publish With Versioning And Audit History.

Step 6

Rule families

Velocity	e.g., 3 different cards used by the same email in 24 hours
Customer Entity	Email/phone reuse, historical approval rates
Shufti's AI	Score thresholds, similar-transaction scores, engine versions
General	Shipping/billing/geo/time/device logic
Industry-specific	Airlines, gaming, hotels, digital goods
Match	Billing name vs. cardholder, postcode vs. city
Payment-method	BIN country, expiry, method, brand
Add-ons	Sanctions/PEP, device fingerprinting, PSD2 exemptions

Priorities & Conflict Resolution

Rules compete by action and priority. The custom actions can be made to win over generic approval/decline when needed (e.g., force step up for a narrow pattern).

Simulation & Safety Nets

- **Run rules on historical data:** total/unique hits | Fraud hits | Decision authority
- **Test a rule** against a specific past transaction.
- **Score investigation** (with ≥6 months' data): Choose a score threshold and see the impact on

  Decline rate | Catch rate | GUDR | Precision

  turning threshold into evidence, not guesswork.

Custom Lists (Allow/Block/Watch)

Instant overrides for

- VIP emails
- Corporate IPs
- Known devices
- Mule emails.
- Compromised cards

CSV bulk-manage

- Hit rate
- Catch rate
- Simulator reports
- Accuracy
- False Positive Ratio

Proactive Alerts

Threshold Alerts

If a rule hits N transactions or X% of traffic in a window.

Change Alerts:

Behavior deviates from baseline (spikes/drops), catching fast attacks (e.g., card testing), and mis-tuned logic early.

Performance KPIs: Measuring What Matters)

- **Precision** (fraud hits / total hits)
- **Catch Rate** (blocked fraud / observed fraud)
- **Game-changer vs. Ineffectual Hits** (retire noisy rules)
- **GUDR** (good user decline rate)
- **Approval/decline distribution by count & value**

Optional Ads-on

Sanctions & PEP Screening	Screen customer names (and addresses) against global watchlists to detect sanctioned or politically exposed persons. Results are returned instantly and can be logged for audits or follow-up actions.
PSD2 exemption	Flag eligible transactions (e.g., low risk, recurring, corporate payments) to request exemptions under PSD2 and reduce Strong Customer Authentication (SCA) requirements. Helps improve conversion while staying compliant..
Device Fingerprinting	Deploy a lightweight browser script to capture advanced device information and assign a persistent device ID (device_id). This enhances fraud detection by identifying anomalies like reused or spoofed devices.

Back Office Visibility

Filter Dashboards

Filter dashboards by period or merchant, compare decline rates, map fraud geographically, and inspect detailed cases and approval rates.

Transactions Search

By device ID, email, descriptors, date; view transaction ID, amounts, IP country, decision, latest status.

Reports

- Real-time overviews of approval rates, traffic trends, approvals/declines, fraud cases (only approved-then-fraud, not already-declined).
- Filters for date & merchant; 12-month retention; pin filters; email or schedule regular delivery (daily/weekly/monthly/quarterly).

Implementation Notes

API. Validation. & Resilience

Required Fields & Responses

Score, decision codes (approved), trans_id, optional device_id, validation hints, error messages, optional liability fields.

Validation Feedback

Per-field ok=true/false flags to fix malformed inputs quickly (e.g., invalid IP/country/timestamps).

Errors & Rate Limiting

Standard 2xx/4xx/5xx; on 429 back off ~10–20s before retry.

Two-way Learning Loop

Uses sync and async updates to ensure continuous model freshness without extra ops burden.

Available via API

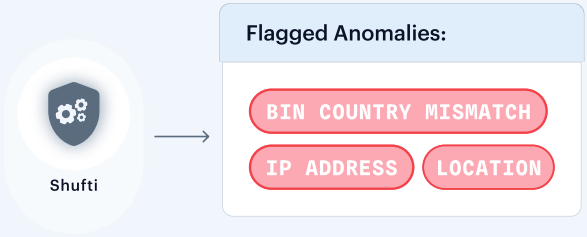
(For Payments and Risk Engineering) and Back Office (for operations). Adopt now, evolve later..

Where You Benefit

Fraudulent Deposit Attempts

A trader tries to deposit funds using a stolen or synthetic credit card.

Value: You can blocks fraud at pre-authorization, reducing chargeback losses and maintaining clean processor traffic.

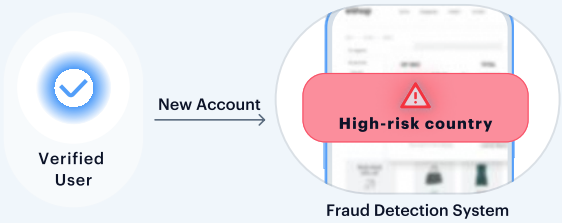


Shufti flags anomalies such as BIN country mismatch, risky email domain, device fingerprint inconsistencies, or IP from a VPN/proxy.

Suspicious Withdrawal Behavior

A verified user initiates **large, rapid withdrawals** to a new bank account in a high-risk country.

Value: Prevents account takeover attempts, mule account payouts, and money laundering through trading accounts.

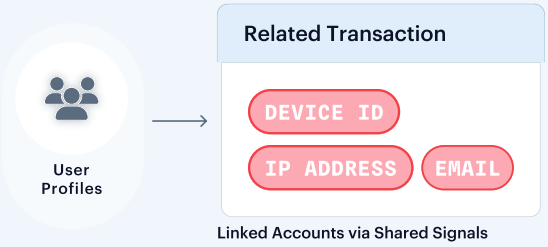


Rules combine velocity checks, device ID tracking, and AML screening.

Coordinated Market Abuse

Multiple accounts execute **synchronized trades around news events**, potentially manipulating FX/CFD spreads.

Value: Supports trade surveillance obligations, helping them detect and stop collusion or manipulative trading behavior.

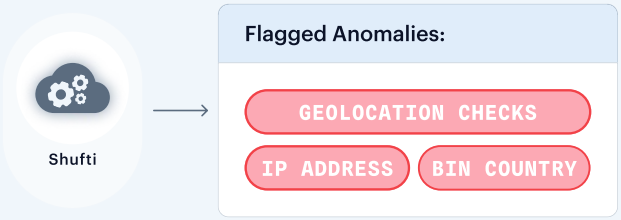


Shufti's "related transaction" logic links accounts through device IDs, IPs, or emails, surfacing suspicious rings.

Cross-Border Payment Risks

A client in Africa or Latin America funds an account via local wallets (e.g., OVO, GCash, PayMaya).

Value: Safely expands into new geographies while maintaining compliance with AML directives.



Shufti enriches transaction data with IP, device, BIN country, and geolocation checks.

Policy Abuse & Bonus Exploitation

Traders create multiple accounts to exploit sign-up bonuses or promotional credits.

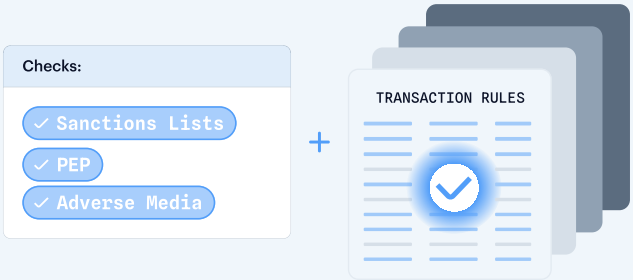
Value: Protects marketing spend and ensures fair use of incentives.

Device fingerprinting and velocity rules detect duplicate identities across accounts.

High-Risk Jurisdiction Screening

Traders create multiple accounts to exploit sign-up bonuses or promotional credits.

Value: Aligned with global AML obligations under ASIC, Mauritius FSC, and FATF standards.



Sanctions/PEP add-on checks combined with transaction screening rules trigger manual review.

What It Means For Your KPIs

Illustrative Scenario

A client executes a **$5,000 EUR/USD trade**:

- Account funded via card issued in Germany, but login IP is from Nigeria.
- The device fingerprint matches a prior account flagged for fraud.
- The email domain is linked to previous suspicious activities.

Shufti's AI flags multiple red signals, lowering the transaction's score below the decline threshold.

Decision: The trade is automatically declined.

If you still processed it and it later resulted in a fraudulent withdrawal or chargeback, an async update would feed the learning loop , preventing similar abuse in future.

Business Impact

Higher Approval Rate

Fewer false declines via better signal and score investigation.

Lower Chargebacks & Costs

Block fraud pre-authorization; clean traffic for issuer.

Faster Investigations

Clear stories, signals, related-transaction linkages, focused dashboards.

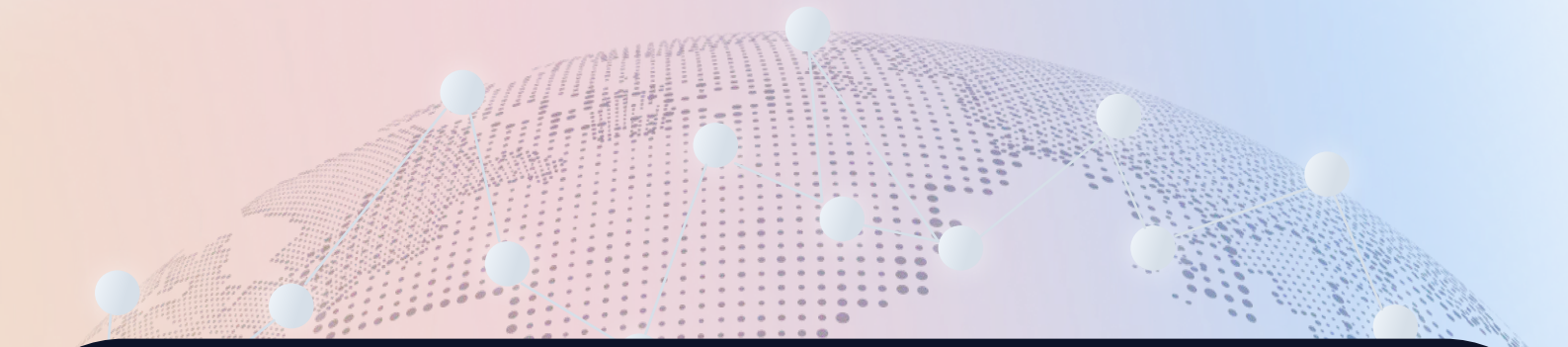
Full Control

Rules, templates, lists, alerts, simulations—adapt posture as your business and adversaries evolve

Shufti

With Shufti, you get a secured and faster way to manage fraud risks.

Empowering your business to thrive in an increasingly digital world.



Ready to take control of your transactions?

Book a Demo

SALES@SHUFTI.COM WWW.SHUFTI.COM