



# Transaction Fraud Monitoring & Decision Intelligence Platform

A next-generation fraud detection solution designed to empower financial institutions with AI-driven intelligence, real-time monitoring, and explainable decision-making capabilities.

## The Growing Fraud Challenge: A Billion-Dollar Problem

Every day organizations process thousands of transactions where fraudsters hide among legitimate customers, exploiting high-volume environments where manual detection is impossible.

### The Scale of Impact:

- \$5.4 trillion lost globally to fraud annually (6% of global GDP)
- 1 in every 100 transactions contains fraudulent elements
- 73% of businesses experienced fraud in the last year

**Detection rate:** Only 56% caught before damage occurs

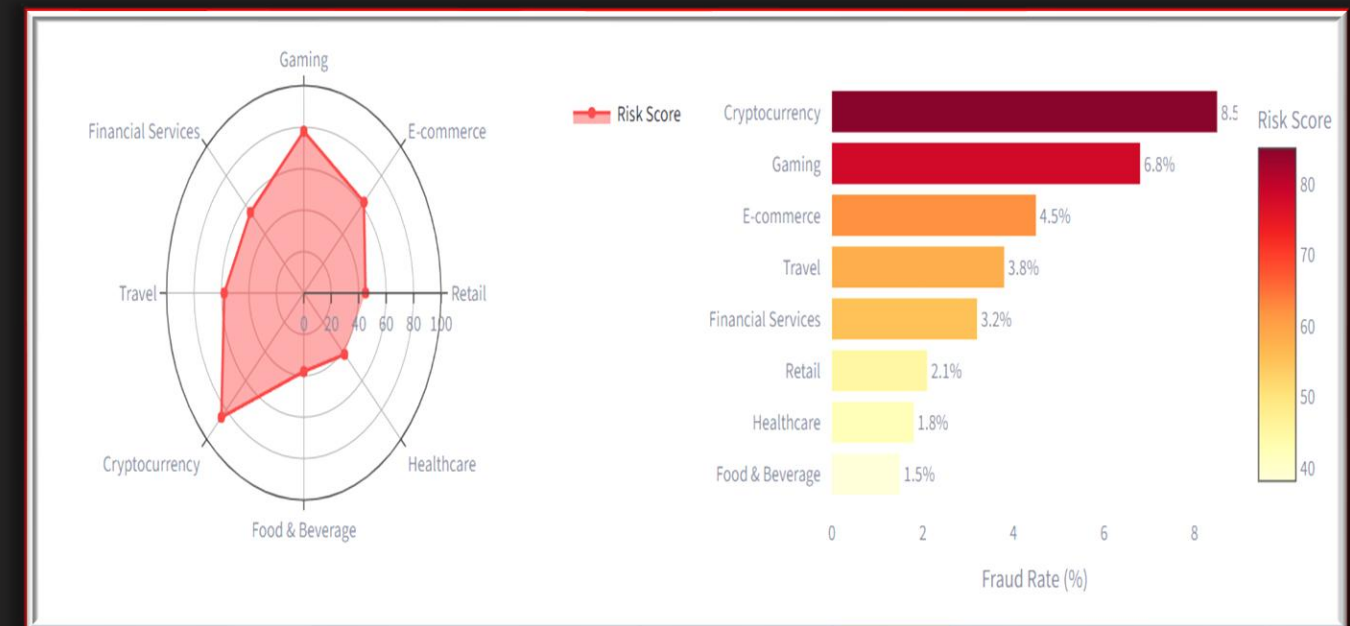
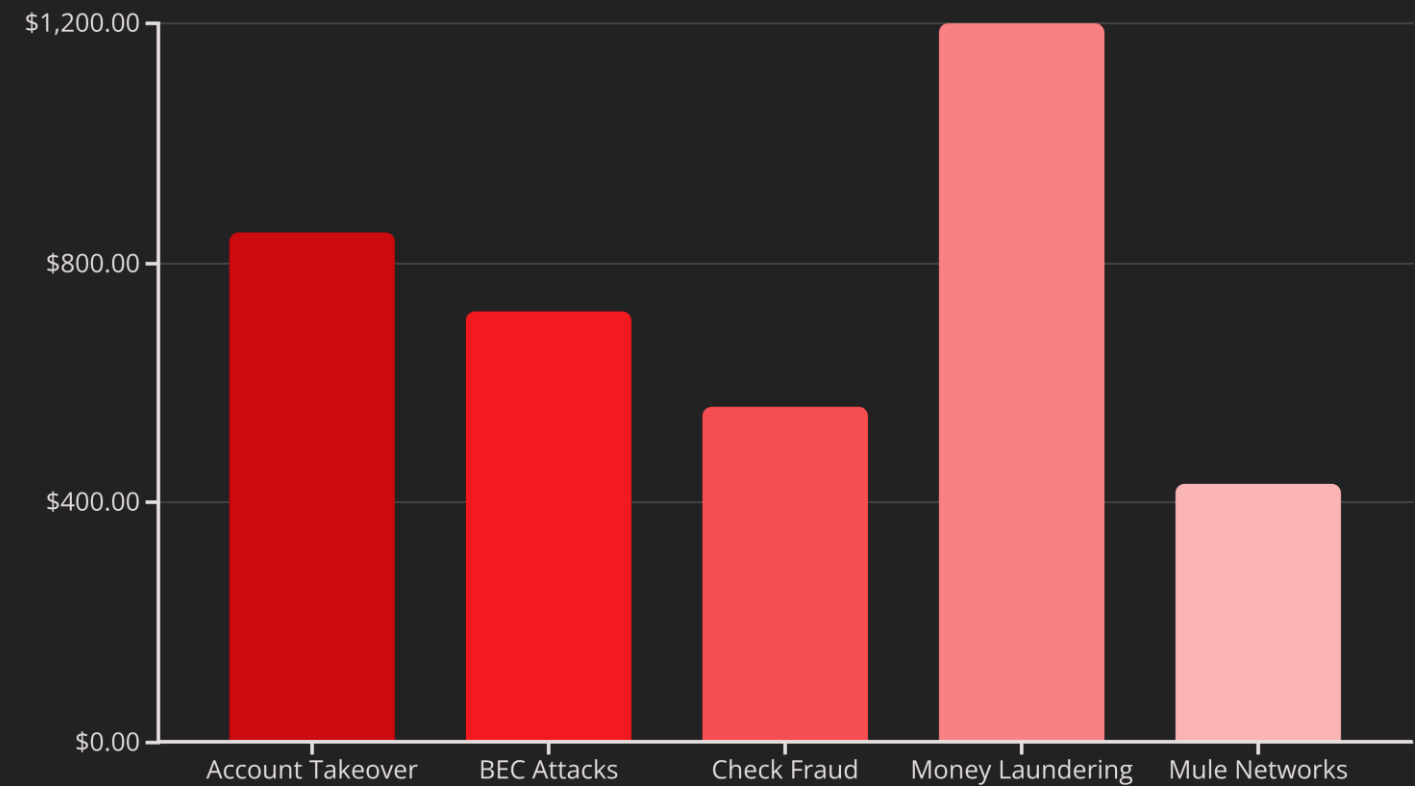
Traditional Methods:

**Volume Overwhelm:** 50,000+ daily transactions make manual review impossible

**Speed Mismatch:** Fraudsters execute in milliseconds; detection takes hours/days

**Pattern Evolution:** New fraud schemes emerge faster than rules can be written

**False Positives:** 95% of alerts are false, causing alert fatigue





# Client Pain Points: Fragmented Systems, High Costs, Poor Outcomes



## Siloed Detection Systems

Banks struggle with separate fraud systems for each attack vector—payroll reroute, BEC, account takeover, money laundering, check fraud, and mule activity—creating blind spots and coordination failures.



## Alert Fatigue & False Positives


Current systems generate 50-70% false positive rates, overwhelming fraud teams with unnecessary alerts, delaying legitimate transactions, and creating significant operational inefficiency and customer friction.



## Black Box Decisions

Poor explainability makes it impossible to justify decisions to regulators, customers, or internal stakeholders. Manual review processes are slow, fragmented, and expose institutions to regulatory risk.





# From Vision to Value: Our Solution Logic

## Vision-Driven Solution Architecture

We architect platforms that push boundaries—built for growth, adaptable to AI/ML innovation, and primed for immediate impact.

Every decision in our design framework answers real market needs: seamless integration, explainability, and audit-ready transparency.

## Catalyst Advisory Philosophy

We enable banks to act decisively, selecting fintech partners that accelerate value and spark differentiation.

Our client-centric mindset is about igniting fast wins now and laying the foundation for long-term transformation.



# Platform Demo: See Intelligence in Action

Experience firsthand how our platform transforms fraud detection from reactive alert management to proactive risk intelligence. The demonstration showcases real-time transaction monitoring, advanced chain analysis visualization, explainable AI decision-making, and configurable risk profiles in action.

1

## Live Transaction Monitoring

Watch the system analyze incoming transactions in real-time, applying AI-powered risk signals across all fraud categories with second response times

2

## Explainability Deep Dive

Review comprehensive SHAP and LIME analysis showing exactly why each decision was made, with full audit trails meeting regulatory standards

3

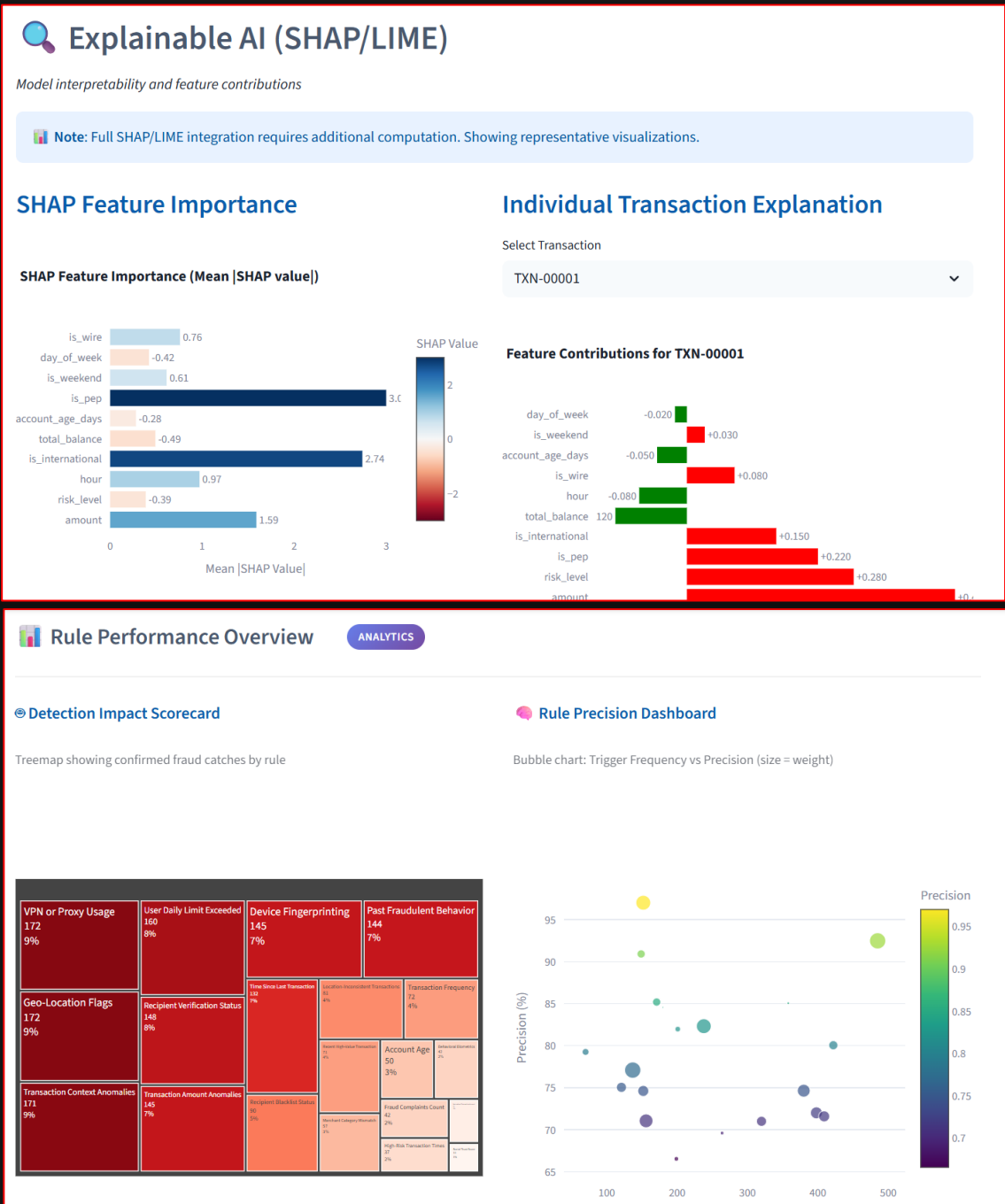
## Configuration & Customization

See how easily the platform adapts to different risk profiles, custom rules and institution-specific requirements without requiring technical expertise

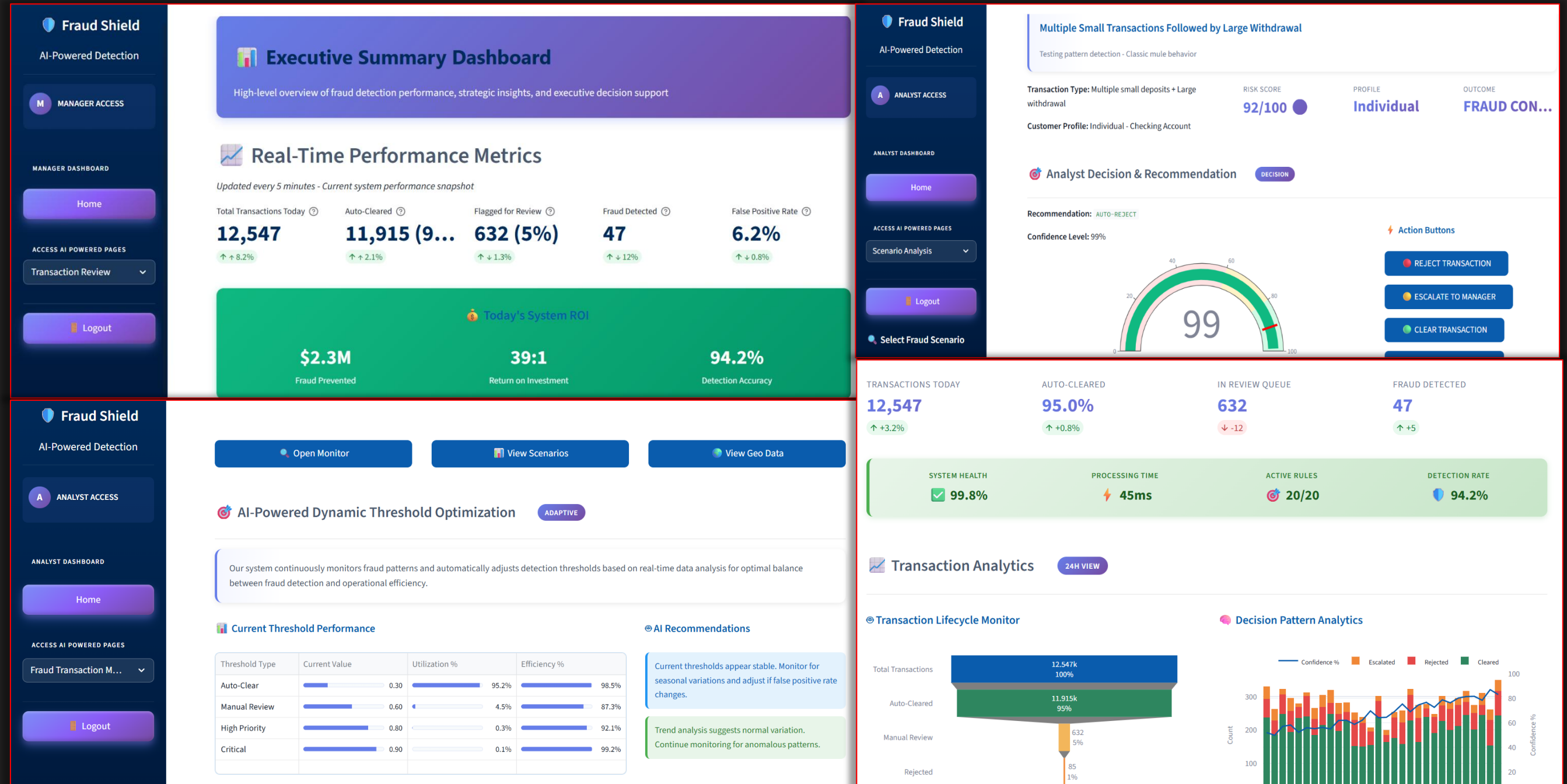
4

## Chain Analysis Visualization

Explore interactive network graphs that reveal hidden connections between accounts, exposing coordinated fraud networks and coordinated fraud rings



# Concept to Reality: Live platform



# Meeting the Market Demand: AI-Driven Fraud Detection



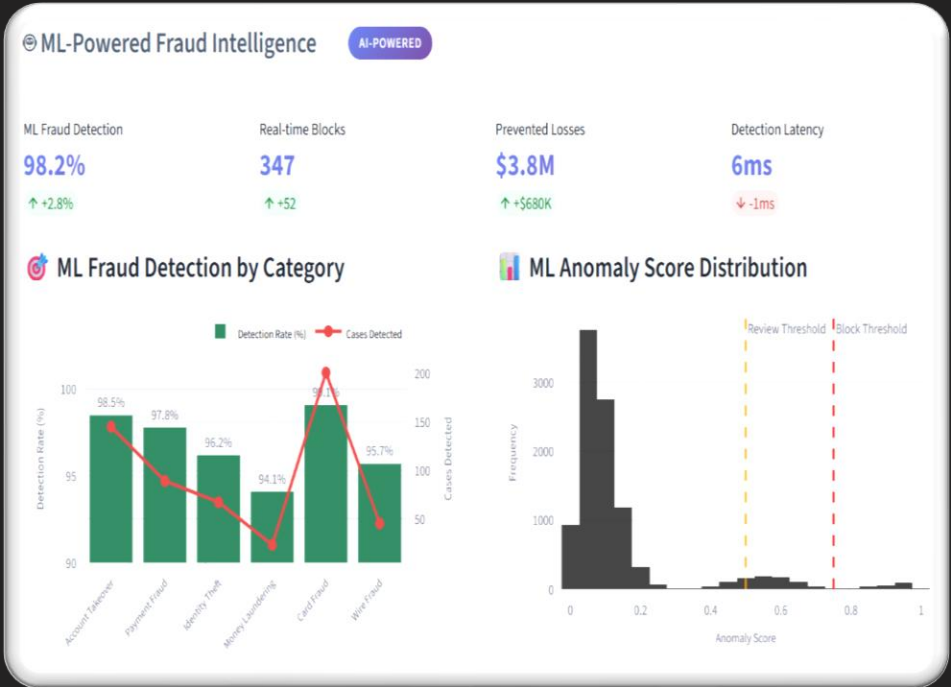
## The Growing Threat

Fraud losses surged past \$40 billion in 2024, with 90% of U.S. companies facing sophisticated, AI-powered fraud schemes that evolve faster than traditional defenses can handle.



## Smart Detection

Our solution leverages cutting-edge AI and machine learning to identify fraud in real-time, continuously adapting to emerging threats and staying ahead of fraudsters.



## Repeatable Revenue Model

This architectural flexibility enables repeated sales across multiple industries and use cases. Each implementation can be tailored while leveraging core components, maximizing both client value and revenue potential.

## Competitive Advantage

In a market demanding smarter, faster fraud defense, our AI-driven solution transforms complex risk into opportunity—empowering clients to prevent fraud proactively while optimizing operational efficiency and compliance.

# AI-Driven Threat Intelligence Platform

### Real-time ML Monitoring

Live model performance and drift detection

Model Accuracy  
**94.3%**  
↑ +1.2%

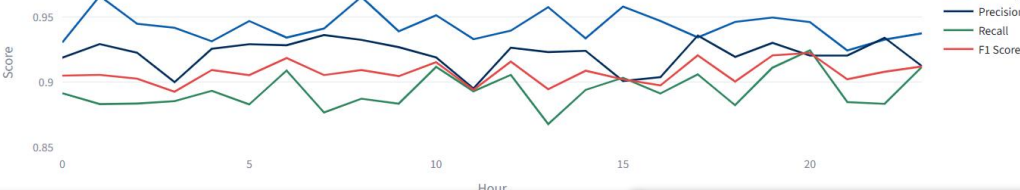
Predictions/Min  
**1,247**  
↑ +156

Avg Latency  
**12ms**  
↓ -2ms

Data Drift Score  
**0.08**  
↓ -0.02

#### Model Performance Timeline

Model Metrics - Last 24 Hours



Accuracy

Precision

Recall

F1 Score

app.py

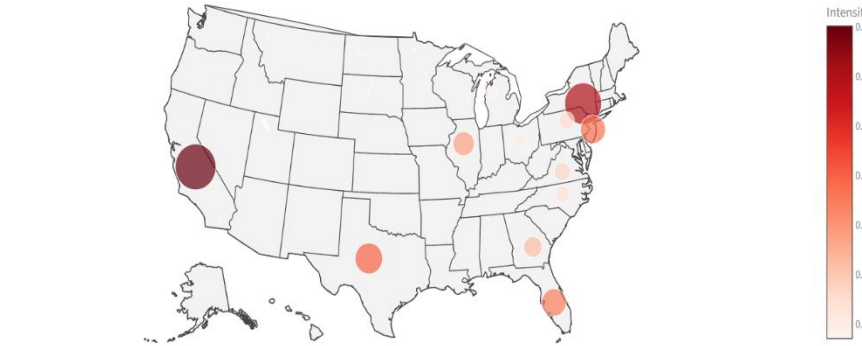
AI\_ML\_Intelligence.py X

```
streamlit_app > pages > AI_ML_Intelligence.py > ...
3117 def render_advanced_metrics(features, colors):
3118     rf = RandomForestClassifier(n_estimators=100, random_state=42)
3119     rf.fit(X_train, y_train)
3120     y_pred_proba = rf.predict_proba(X_test)[:, 1]
3121
3122     col1, col2 = st.columns(2)
3123
3124     with col1:
3125         # F1 score at different thresholds
3126         st.markdown("### F1 Score Optimization")
3127
3128         thresholds = np.linspace(0, 1, 100)
3129         f1_scores = []
3130
3131         for threshold in thresholds:
3132             y_pred = (y_pred_proba >= threshold).astype(int)
3133             if len(np.unique(y_pred)) > 1:
3134                 f1 = f1_score(y_test, y_pred)
3135             else:
3136                 f1 = 0
3137             f1_scores.append(f1)
3138
3139         optimal_idx = np.argmax(f1_scores)
3140         optimal_threshold = thresholds[optimal_idx]
3141         optimal_f1 = f1_scores[optimal_idx]
3142
3143         # Enhanced hover texts for F1 optimization curve
3144         f1_hover_texts = []
3145         for thresh, f1 in zip(thresholds, f1_scores):
3146             # Distance from optimal
3147             dist_from_optimal = abs(thresh - optimal_threshold)
3148
3149             if thresh == thresholds[optimal_idx]:
3150                 status = "🏆 OPTIMAL THRESHOLD"
```

Geolocation Threat Map

USA

Device locations remotely triggered across USA using VPN/Proxy



Highest VPN Fraud  
**California**  
↑ 145 cases

Second Highest  
**New York**  
↑ 132 cases

Third Highest  
**Texas**  
↑ 98 cases

app.py

chain\_analyzer.py X

```
app > services > chain_analyzer.py > ...
64 class ChainAnalyzer:
281 def calculate_suspicion_score(self, nodes: List[TransactionNode],
291     # Base score by pattern type
292     pattern_base_scores = {
293         "credit_refund_transfer": 0.7,
294         "layering_consolidation": 0.8,
295         "rapid_reversal": 0.6
296     }
297     score = pattern_base_scores.get(pattern_type, 0.5)
298
299     # Adjust for chain length (longer chains are more suspicious)
300     if len(nodes) >= 4:
301         score += 0.1
302     if len(nodes) >= 5:
303         score += 0.1
304
305     # Adjust for speed (faster chains are more suspicious)
306     if time_span_hours < self.RAPID_TIMEFRAME_HOURS:
307         score += 0.1
308     if time_span_hours < 2:
309         score += 0.1
310
311     # Check for varying counterparties (more suspicious)
312     unique_counterparties = len(set(n.counterparty_id for n in nodes))
313     if unique_counterparties >= 3:
314         score += 0.1
315
316     # Check for small transaction amounts (testing behavior)
317     small_tx_count = sum(1 for n in nodes
318         if n.amount < self.SMALL_TRANSACTION_THRESHOLD)
319     if small_tx_count >= len(nodes) * 0.5:
320         score += 0.05
321
322     # Cap at 1.0
323     return min(1.0, score)
```

AI & Machine Learning Intelligence

Advanced machine learning analytics and model intelligence for fraud detection

Neural Networks

Ensemble Models

Model Performance

Explainable AI

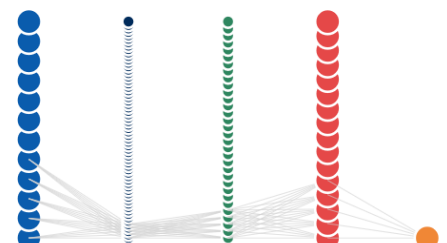
Real-time Monitoring

Feature

### Neural Network Architecture & Activations

Deep learning model structure and activation patterns

Neural Network Architecture



Input Layer

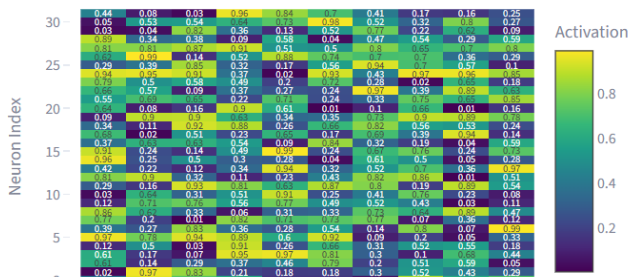
Hidden Layer 1

Hidden Layer 2

Hidden Layer 3

Output Layer

Layer Activation Patterns (Hidden Layer 2)



Activation

app.py

account\_takeover\_rules.py X

```
app > services > account_takeover_rules.py > ...
103 def create_suspicious_phone_change_transfer_rule(
122     name = rule_name or f"suspicious_phone_change_transfer_{max_hours}h"
123
124     def condition(tx: Dict[str, Any], ctx: Dict[str, Any]) -> bool:
125         # Only check outgoing transfers
126         if not ctx.get("is_outgoing_transfer", False):
127             return False
128
129         # Check for suspicious phone changes
130         suspicious_count = ctx.get(f"suspicious_phone_changes_{max_hours}h", 0)
131         return suspicious_count > 0
132
133     return Rule(
134         name=name,
135         description=f"Outgoing transfer after suspicious phone/device change - likely
136             condition_func=condition,
137         weight=weight
138     )
139
140 def create_first_transfer_after_phone_change_rule(
142     rule_name: str = None,
143     weight: float = 3.0
144 ) -> Rule:
145     """
146     Detect the first outgoing transfer after a phone change.
147
148     The first transfer after a phone change deserves extra scrutiny,
149     especially if combined with other risk factors.
150
151     Args:
152         rule_name: Optional custom rule name
153         weight: Rule importance weight
154     """
```



# Business Value and Opportunity



## Standalone Capability

Key benefits: The platform delivers measurable financial and operational gains from day one. Prevents high-value losses saving up to \$47K per fraud while reducing investigation time by 95%. With fast deployment, organizations move from lengthy advisory projects to solution-driven execution.



## Managed Monetization Models

Proactively shields from regulatory and reputational damage by ensuring full AML and compliance adherence. Prevents \$1.2M+ in potential fines, blocks sophisticated frauds averaging \$100K–\$200K per attack, and maintains a 100% auditable trail for every investigation. Beyond protection, our scalable SaaS and enterprise licensing model enables recurring revenue through continuous access, system upgrades, and support—turning risk mitigation into a sustainable business advantage.



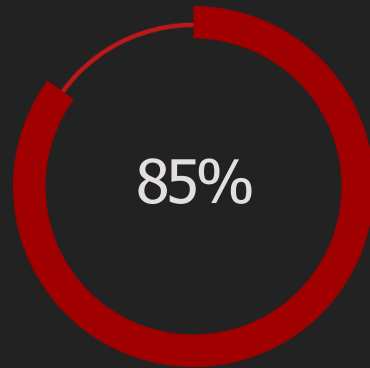
## Assessment & Advisory Expansion

Effortlessly scale to manage 50k+ daily transactions with real-time response under 2ms, enabling enterprise-grade performance. With 13 pre-configured fraud patterns and self-learning AI, protection evolves continuously without manual updates. Each deployment not only enhances client defense but uncovers operational inefficiencies, fueling new consulting opportunities.

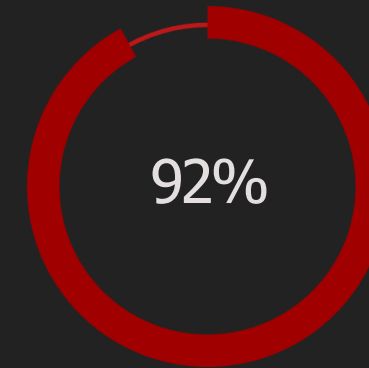
# Client Benefits: Transform Fraud Detection Effectiveness

Banks implementing our platform experience dramatic improvements in fraud detection accuracy, operational efficiency and risk management effectiveness within the first day of deployment.

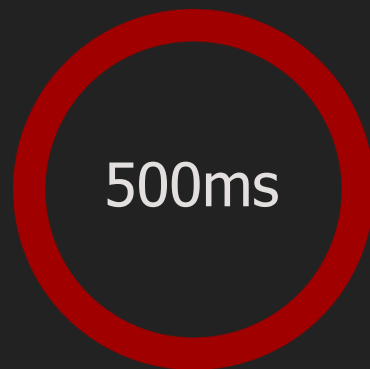
The combination of AI-driven intelligence, comprehensive coverage, and explainable decision-making creates a new standard for fraud prevention excellence.



**Reduction in False Positives**  
Cut alert fatigue and operational productivity



**Fraud Detection Rate**  
Catch threats missed across other solutions



**Average Response Time**  
Real-time decisions without friction



**Audit Trail Coverage**  
Complete explainability for every decision

# Advanced Fraud Protection



## Dormant Account Surge Protection

AI detects unusual large transfers from inactive accounts

- Advanced behavioral analytics identify transfers exceeding account-level baselines and trigger automated risk scoring.
- Recipient verification logic validates ownership and cross-checks historical trust factors.
- Suspicious events auto-escalate for review or immediate block before fund settlement.



## Test-and-Drain Prevention

Blocks Large Withdrawal after detecting probe patterns

- Sequence-aware algorithms detect micro-transaction bursts that precede major withdrawals.
- Velocity and progression tracking flag unusual accumulation behavior.
- Automated hold policies pause withdrawals pending secondary authentication.



## Payroll Redirect Shield

Prevents fraudsters from redirecting legitimate payroll deposits.

- Authenticates changes to employee direct deposit information.
- Flags changes made from unusual IP addresses or devices.
- Requires multi-factor authentication for sensitive payroll modifications.
- Compares new banking details against known fraud patterns.



## Money Mule Network Detector

Identifies individuals involved in laundering illicit funds.

- Analyzes transaction patterns for frequent, small deposits followed by large transfers.
- Maps recipient networks to uncover connections to known fraud rings.
- Monitors accounts for sudden changes in activity inconsistent with historical behavior.
- Uses geospatial analysis to detect mule activity across different regions.



## Micro-Deposit Interceptor

Blocks fraudulent account verification attempts using small deposits.

- Detects high volumes of micro-deposits to newly created or suspicious accounts.
- Identifies patterns of rapid deposit and withdrawal, indicating account testing.
- Analyzes the origin and destination of micro-deposits for unusual correlations.
- Automated rules block accounts participating in micro-deposit fraud at scale.



## Transaction Chain Analyzer

Uncovers complex fraudulent schemes by tracing transaction paths.

- Visualizes money flows across multiple accounts and institutions.
- Identifies circular transactions or sudden diversions from normal patterns.
- Pinpoints central nodes in fraud networks for targeted intervention.
- Applies graph analytics to detect hidden relationships and suspicious clusters.



# Advanced Fraud Protection



## Account Takeover Fortress

Instant lockdown for SIM Swaps and compromised credentials

- Adaptive authentication models detect login velocity and geo-anomalies across devices.
- Real-time credential reuse detection flags breaches before fraudulent access occurs.
- Step-up verification and multi-factor enforcement neutralize unauthorized login attempts.



## Duplicate Check Eliminator

Catches duplicate check deposits for multiple accounts or banks

- Identity graph analytics correlate PII patterns to spot fabricated profiles and mismatched KYC data.
- Cross-channel data matching and velocity controls highlight unnatural identity reuse.
- AI-based link analysis uncovers clusters of synthetic entities tied to fraud rings.



## Vendor Fraud Gatekeeper

Cooling period for all beneficiary changes with payment blocks

- Session behavior monitoring detects deviations from typical user patterns post-login.
- Risk-scored email/IP analysis identifies spoofed communication sources.
- Transaction-level policy rules auto-block unauthorized fund movements triggered after phishing access.



## Geographic Risk Controller

Real-time blocking of payments to sanctioned or high-risk jurisdictions

- Real-time transaction scoring combines device fingerprints and merchant reputation data.
- Geo-behavioral profiling flags impossible spending locations or unseen devices.
- Adaptive limit rules auto-reduce risk exposure for high-fraud channels and regions.



## Account Manipulation and Bulk Payment Guardian

Stops mass beneficiary schemes before insider fraud escalates

- Access analytics track role-based permissions and flag abnormal privilege use.
- Audit trail reconciliation detects unauthorized data exports or configuration changes.
- Automated alerts notify compliance teams when insider activity breaches policy thresholds.



## Money Laundering & Round-the-Clock Sentinel

AI adjustments to risk thresholds 3x higher during non-business hours

- Network analysis maps multi-hop fund flows to identify layered and integrated transactions.
- Risk scoring combines beneficiary linkage and jurisdiction exposure for AML compliance.

# Platform Highlights: Intelligence That Delivers Results

## Real-Time Risk Scoring

Dynamic risk assessment with multi-dimensional scoring algorithms that evaluate transactions across behavioral, contextual, and network indicators simultaneously.

## Regulatory Compliance

Built-in audit trails, compliance reporting, and documentation capabilities ensure alignment with regulatory requirements with complete decision transparency



## Advanced Chain Analytics

Visualize complex fraud networks with interactive graph analytics, identifying mule accounts and coordinated attack patterns across 24-hour transaction windows.

## Comprehensive Explainability

AI built-in explainability charts using LIME and SHAP ML methodologies provide complete transparency into model decisions for regulatory, doctrine, and stakeholder use.

## Flexible Configuration

Adapt to your institution's risk appetite with configurable detection profiles, custom rule sets, and adjustable thresholds that balance security with user experience.

# Partner With Us to Transform Fraud Detection

This platform represents a strategic opportunity delivering unprecedented value. By combining sophisticated AI technology with financial expertise, we can transform how institutions detect, prevent, and respond to fraud.

## Schedule Your Deep Dive

Let's discuss how this platform fits your client engagement strategy and explore customization opportunities for specific bank requirements

## Pilot Program Opportunity

Deploy with a select client bank to demonstrate immediate impact and build compelling case studies for broader rollout across your client base

## Strategic Partnership Discussion

Explore licensing models, revenue sharing structures, and long-term collaboration frameworks that align with growth objectives

**Contact:** Ready to transform fraud detection for your clients? Let's schedule a detailed technical review and business discussion to move forward together