



SHI AI Fraud Detection

Real-time, explainable AI fraud prevention for public and private sector organizations.



Fraud is more sophisticated, more coordinated, and more damaging than ever before. From synthetic identities and collusive vendor networks to benefits abuse and insider threats, bad actors are leveraging advanced tactics that rules-only systems can't detect. Meanwhile, fraud teams are overwhelmed by false positives, compliance requirements tighten, and financial losses continue to mount.

SHI's AI Fraud Detection service redefines fraud prevention — shifting from reactive investigation to proactive, real-time defense. Powered by GPU-accelerated graph neural networks (GNNs) and XGBoost models, the solution uncovers hidden relationships, anomalies, and fraud rings that traditional rule-based systems miss and makes real-time decisions to stop emerging fraud tactics before they cause damage.

What does this mean for you? Faster detection, audit-ready transparency, and operational efficiency to protect funds, reduce operational strain, and maintain public trust — all backed by SHI's proven expertise in AI deployment and integration.

What makes AI fraud detection different?

- **Real-time detection:** Flag and stop fraudulent activity before losses occur.
- **Explainable AI (XAI):** Every decision is traceable and auditable, ensuring regulatory confidence.
- **Reduced false positives:** Analyst teams focus on high-value cases, not noise.
- **Fast time-to-value:** AI Lab Fast Start delivers proof in 2-3 weeks using your data.
- **Enterprise-grade scalability:** Containerized, Kubernetes-ready, and cloud/hybrid compatible.

Outcomes that matter

- Up to **80%** reduction in targeted fraud losses.
- Up to **60%** decrease in false positives.
- **5-10x** ROI through loss prevention, efficiency, and recovery.
- **43%** increased efficiency within fraud teams.
- Stronger compliance posture and audit readiness.

Key industry use cases

- **Banking/Fintech:** Credit card fraud, account takeovers, synthetic identity creation, and mule accounts.
- **Public sector/Government:** Procurement fraud, benefits abuse, and insider threats.
- **Healthcare:** False claims, provider collusion, and billing manipulation.
- **Higher education:** Financial aid fraud, falsified credentials, and duplicate applications.
- **Retail/Ecommerce:** Returns abuse, loyalty program exploitation, and promo fraud.
- **Insurance:** Staged or duplicate claims and organized fraud rings.

SHI AI Fraud Detection

Real-time, explainable AI fraud prevention for public and private sector organizations.

Why SHI

SHI is not just a global IT solutions provider; we are your AI transformation partner. Our AI Lab infrastructure, in partnership with NVIDIA, is purpose-built for enterprise-grade ideation, experimentation, and adoption. This aligns directly with our strategic approach: Imagine, experiment, adopt. We empower organizations to imagine what's possible with AI, experiment in secure, scalable environments designed for rapid prototyping and production rollout, and adopt solutions with confidence – backed by our deep expertise in infrastructure, data governance, and enterprise AI.

Whether you're a CIO seeking strategic clarity or a developer building the next-gen AI app, SHI brings the technical depth and operational rigor needed to succeed. We help you navigate complexity, reduce risk, and unlock real business value.

- **Outcome-first approach:** KPIs aligned and defined from day one.
- **AI solution prototyping:** Proof of value in weeks, not months.
- **Full-stack delivery:** From model training to platform and MLOps integration.
- **Cross-sector expertise:** Proven in regulated, mission-critical environments.
- **Trusted partner ecosystem:** NVIDIA, OEMs, NCPs, and leading security platforms.

How AI fraud detection works

- **Data ingestion:** Securely process structured, unstructured, and streaming data feeds.
- **Feature engineering:** Extract transactional and relationship-based signals for modeling.
- **Hybrid modeling:** SHI's fraud detection engine combines two powerful hybrid modeling techniques. These techniques operate together to detect both complex fraud rings and isolated suspicious behavior, giving your team a comprehensive, real-time view of risk – without needing a data science degree to understand how it works:
 - Graph neural networks (GNNs) uncover hidden relationships between entities – like collusive vendors or synthetic identities – by analyzing how data points connect.
 - GNNs detect hidden fraud rings, collusion, and multi-party schemes.
 - XGBoost delivers high-precision scoring for individual transactions, helping flag anomalies with speed and accuracy.
 - XGBoost delivers high-precision scoring for individual transactions.
- **Real-time serving:** NVIDIA Triton Inference Server scores transactions in milliseconds.
- **Case investigation:** React-based dashboards with graph visualizations empower analysts.
- **Continuous learning:** Models auto-retrain to adapt to new fraud patterns.

SHI AI Fraud Detection

Real-time, explainable AI fraud prevention for public and private sector organizations.

Personas and benefits

SHI aligns technical outcomes with business priorities across every stakeholder.

Persona	Benefit	Why it matters	Business outcome
CIO/CTO	Scalable, secure fraud detection	Future-proof against evolving threats	Lower infra cost, faster capability deployment
CISO/Risk	Real-time detection and XAI	Stronger proactive risk management	Reduced exposure, better compliance scores
Compliance Officer	Audit-ready decisions	Simplify AML/KYC/FISMA requirements	Faster audits, fewer penalties
Fraud Ops Leader	Fewer false alerts, visual mapping	Higher investigative efficiency	Faster closure rates, better detection of schemes
Program Owner	Detect benefits/procurement fraud	Protect funds	Measurable fraud reduction, public trust
Finance Exec	Clear ROI	Demonstrate financial benefit	Significant loss reduction, budget reallocation

Business impact in action

A state benefits agency engaged SHI for a 2-week AI Lab validation. Using historical and real-time data, the system identified a collusive vendor ring and a duplicate beneficiary scheme. Within 6 weeks of pilot deployment, there was a reduction of:

- Fraudulent payouts.
- TTI: Time to investigation resulting in annualized savings.
- Audit response time (ART) – From weeks to hours.

Engagement model

- AI solution prototyping: Validate with your data in 2-3 weeks.
- Integration and tuning: Connect to live systems, set thresholds, and train users.
- Production readied: Scale to multiple fraud types and departments.
- Continuous optimization: Including retraining, performance reviews, and new use cases.

Scan to learn more



Contact us

Book your AI Lab engagement today to see your fraud risks, model performance, and ROI forecast before committing to full deployment.

Speak to an AI expert. Contact us at AI@SHI.com.

Learn more at SHI.com/AI.

SHI International Corp. SHI.com [888-764-8888](tel:888-764-8888) [3](https://www.linkedin.com/company/shi)