AI Fraud Detection Readiness Checklist For Financial Institutions

Many financial institutions (FIs) take a reactive approach to fraud prevention and detection. They review past data to make connections, then learn from their gaps and inefficiencies to better prepare for the future.

The problem with that approach is that, as data prevention methods are evolving, fraudster attack methods are evolving as well. It's not enough to prepare for the last war; you must also prepare for the next battle, the incident you cannot anticipate in advance. This is the role that artificial intelligence (AI) and machine learning (ML) play in fraud detection. Despite AI's numerous benefits in helping FIs become forward-looking, many financial institutions simply aren't structurally prepared to put Big Data and AI to work.

Use this complimentary AI Fraud Detection Readiness Checklist to help you assess your FI's current preparedness to adopt AI fraud prevention and detection tools.

- Understand your current fraud landscape
- Review existing fraud detect methods
- Explore modern frameworks for fraud management
- Discover how to deploy AI fraud detection solutions

Understand Your Current Fraud Landscape

- [ ] Does your corporate culture approach fraud as a significant business risk? If not, a shift in mind-set should be your first priority.
- [ ] Recognize and catalog the types of technology, tools, or channels that put your business or industry at risk. (e.g. automatic refunds, self-service for opening new accounts, etc.)
- [ ] Take stock of your customer touchpoints and how fraud can occur through each one. (e.g. call centers, friend referrals, account openings, account logins, social media, transactions, etc.)
- [ ] Identify how you want your business to grow in terms of fighting fraud.

Review Existing Fraud Detection Methods

- [ ] Evaluate your current risk profile and the technologies already in use to detect and prevent fraud.
- [ ] Will these existing solutions scale with your business?
- [ ] Analyze potential fraud attack vectors and align how current technology is helping to promote fraud detection and prevention.
- [ ] To address inefficiencies, review the data you are collecting and "feeding" into your current fraud prevention and detection tools.
- [ ] Document the type(s) of data that are not currently being collected, but could be beneficial in detecting or preventing fraud.
- [ ] Identify the tools and technology that could be useful in collecting the types of data needed to strengthen fraud prevention efforts.

A Modern Framework for Fraud Management: What Leading High-Growth Organizations Have in Place to Manage Digital Fraud

- [ ] Device intelligence to detect manipulated devices and emulators
- [ ] Rules engine to detect anomaly patterns and implement business rules quickly and easily
- [ ] Machine learning (specifically unsupervised machine learning) to eliminate overhead associated with data training and frequent re-training
- [ ] Linkage analysis and case management for faster and more accurate fraud investigation
- [ ] Consortium database that gathers fraud intelligence across different industries and geographies for more robust fraud detection

Discover How to Deploy AI Fraud Detection Solutions for Rapid Growth and Success

- [ ] Identify how AI fraud detection solutions adapt to your current systems and tools.
- [ ] Apply a machine learning model in a way that deploys quickly and allows you to see an immediate ROI.
- [ ] Review data sources (e.g. siloed channels) and examine your approach to bring disparate data systems together to create a single source of truth. Having all data in a single place allows AI fraud detection solutions to do their best work.
- [ ] Establish cooperation between cybersecurity and risk management teams, as the two departments are increasingly overlapping.
- [ ] Think through your fraud analytics to identify strengths and opportunities, including but not limited to:
    - o Data governance structure and processes
    - o Data quality
    - o Data utilization
    - o Data analysis
    - o Technology infrastructure
- [ ] After deployment, deploy adversary emulation attacks against your enterprise to validate your cybersecurity controls are working and confirm your implementation. Even the best technology can't defend you if it's misconfigured.