



Emerging Technology in Financial Crime Compliance

Sriram Narasimhan^a

^a*LTIMindtree*

Abstract

Banks and Financial services are evolving rapidly with increased adoption of technology. With this evolution comes increase in financial crime. The methods used for financial crime have become more sophisticated and complex. The rule based applications used to combat financial crime are inadequate and banks are looking at using emerging technologies like machine learning to combat financial crime.

The article addresses the use cases of financial crime compliance where emerging technology and machine learning can be used from the perspective of operational efficiency, risk reduction and enhanced compliance. We are also seeing increased interest in this space from regulators and government entities. Many product companies have embraced the use of emerging tech and artificial intelligence in financial crime compliance and the article also addresses how algorithms can learn from historical data, identify patterns and make predictions to assist financial crime compliance.

Keywords: Financial Crime, Compliance, Artificial Intelligence, Machine learning, Fraud detection

1. Introduction

At the outset, the banking and financial services sector is faced with an avalanche of advanced financial crime methods and has led to banks thinking about adoption of emerging tech, AI and Machine Learning in combatting financial crime. While the technology product firms have embraced these innovations to a large extent banks are viewing this with cautious optimism as given the stringent regulations and the substantial fines by the regulator would mean necessitate getting the implementation of emerging tech right in this space.

However, As per the World Economic Forum financial services firms have spent 35 billion on AI till 2023 and it is going to rapidly increase with advent of Generative and Agentic AI.

In India, the RBI Free AI framework guidelines and SEBI role in utilizing AI for fraud detection AI are opening the doors for innovation in this space.

The FATF (Financial Action Task Force), the volume of fraudulent transactions is estimated to be 2% to 5% of the total GDP.

The combination of financial crime being more sophisticated and the regulator signalling the use of emerging technology, AI and Machine Learning has led to increased adoption in this space for specific use-cases like fraud detection, anti-money laundering, KYC and Sanctions Screening.

Furthermore, there are limitations to existing rule based applications and technology and are increasingly ineffective in combatting financial crime. Most of these techniques are reactive and not real-time and there are numerous false positives which increases the workload of the bank operations team.

2. Financial Crime, Anti Money Laundering and Fraud Detection

Financial crime compliance encompasses a series of policies and procedures that institutions like banks, investment firms, asset managers, and insurance companies must implement to detect and prevent financial criminal activities. The regulatory framework outlines various obligations aimed at ensuring responsible conduct. Key requirements include conducting risk assessments on potential threats, performing customer due diligence regarding identities and

business relationships, implementing enhanced due diligence for high-risk clients, continuously monitoring customer interactions and transactions, reporting suspicious activities, and maintaining comprehensive records related to customer due diligence.

Fraud detection refers to recognizing fraudulent actions or attempts related to money laundering or theft.

Regulatory adherence concerning financial crime risk management remains essential for banking institutions. Many organizations still find managing financial crime risks complex and inefficient.

3. Advancement in AI and ML

Turing's predictions in 1950 laid a foundational understanding for AI and the 1990 and 2000 saw the development of neural networks in financial services. The pervasiveness of data and increase in computing power have seen the advancement of AI and ML in today's context.

Considerable investments have been made by nations to harness the benefits of AI. Advances in Computer Vision, ML and NLP have enabled AI to perform complex tasks. The field of Generative AI has seen great progress with the development of Large Language Models (LLMs) Quantum AI using the properties of Qubits might surpass the limitations of classical AI by solving problems which could not be solved due to computational constraint.

AI that proactively makes decisions on its own will revolutionize the impact it has on corporations. Robotic Process Automation coupled with ML have given rise to Agentic AI and Agentic AI has systems composed of specialized agents that operate independently, each handling specific tasks.

4. Use Cases of AI in Financial Crime and AML – The role of AI in FCC

There are various areas in the Financial Crime value chain which are seeing increased adoption of AI and emerging technology including Fraud Detection and Transaction Monitoring, Enhanced Due Diligence and KYC, Suspicious Activity Reporting, Sanctions Screening and PEP Screening.

Fraud Detection and Transaction Monitoring: Agentic AI systems can detect fraudulent transactions and anomalies at real-time. Supervised learning and classification algorithms train on fraudulent data to classify transactions.

EDD and KYC: Banks use Identity verification and risk scoring for KYC using Computer Vision and Facial recognition. Enhanced Due Diligence is a set of procedures to assess customers based on their risk profiles. Knowledge graphs and Graph Neural Networks for mapping complex relationships, risk profiling are used in EDD.

Generation of SARs: Banks and financial services firms produce SARs to alert regulators on potential suspicious transactions. GenAI can be leveraged to generate these reports and NLP can be used to process the description on these reports to route it to law enforcement agencies.

Sanctions Screening and PEP: AI Agents uncover hidden relationships between PEP and Relatives and Close Associates and for entities which are Sanctioned through multilingual and social analysis and processing with Named Entity Recognition and social media analysis with graph classification.

5. Regulators Adoption of AI in Financial Crime Compliance over the last few years

Reserve Bank of India

RBI has developed a Digital Payments Intelligence Platform which is Centralized fraud intel and real-time risk scoring. It is a national intelligence-sharing and fraud account repository platform for all digital transactions in India. It has enabled Fraud detection across the payment ecosystem and the Collaborative AI-powered fraud detection that identifies suspicious patterns across banks, payment providers, and digital wallets in real-time or in T+1 batches. RBI also launched an Artificial Intelligence (AI) and Machine Learning (ML) based model, namely MuleHunter, to prevent and mitigate digital fraud by using mule accounts.

Additionally, RBI FREE-AI framework - the Reserve Bank of India's guidance for how AI should be responsibly adopted, governed, and deployed in India's financial sector.

Financial Action Task Force Report in July 2021 – Opportunities and Challenges of New Technologies for AML/CFT

Digital Identity Solutions that can enable non-face-to-face customer identification/verification/authentication and updating of information

AI/ML Technology-based Solutions that can be applied to big data can strengthen ongoing monitoring and reporting of suspicious transactions

Natural Language Processing that can support more accurate, flexible, and timely analysis of customer information

6. Emerging Technology in the Financial Crime and Compliance space

1. Classical AI and Machine Learning Models

Supervised and unsupervised learning models detect patterns that rules-based systems miss, improving the precision of alerts in fraudulent transaction detection.

Random Forest/XGBoost – This algorithm is generally used for classification tasks which are trained on historical data labelled as ‘fraudulent’ and ‘non-fraudulent’.

Support Vector Machine – This algorithm flags anomalies by creating a ‘hyperplane’ – boundary around normal data points and flags the outliers as anomalies to identify ‘fraudulent’ transactions.

K-Means clustering groups similar transactions or behaviours to detect anomalies.

Product companies typically use a champion challenger model where one new model challenger model replaces the champion model if the performance of the model improves with additional data or new features.

2. Quantum Computing

For highly imbalanced data sets, quantum computing is used to more accurately identify fraudulent transactions. Classical machine learning based predictions and classifications are good but has limitations when it comes to highly imbalanced data. In such scenario they often struggle to have better Precision and Accuracy and could lead to False Positives and False Negatives. We use Quantum Support Vector Machine algorithm for the Transaction monitoring / Fraud Detection use cases that is based on the classification of labeled data. Quantum Machine Learning (QML) leverages quantum mechanical

phenomena like Superposition and Entanglement, which helps QML models uncover the hidden patterns.

3. Generative AI

Generative Adversarial Networks is used to create synthetic data to improve the accuracy of the predictions as well. Also Generative AI can be used to automatically generate Suspicious Activity Report and NLP is used to process the SAR reports and route it downstream entities as well..

4. Fuzzy Logic

AI-driven fuzzy matching identifies near-match names against sanction lists consolidating identities derived from diverse sources seamlessly functioning together

5. Knowledge Graphs and Ontology

To combat modern fraud, banks and financial institutions must adopt intelligent, interconnected, and autonomous systems that leverage AI for fraud detection. This entails:

Ontology: It defines the semantic structure of financial entities such as customers, accounts, transactions, vendors, as well as their relationships. It enables systems to understand meaning, not just data.

Knowledge Graphs: These map real-time relationships between entities. For example, a graph can show how a customer is linked to multiple accounts, vendors, and geographies. It helps detect unusual patterns, such as a customer suddenly transacting with high-risk countries.

6. Computer Vision

For KYC, facial recognition can be used to detect customer's identity to prevent fraud during onboarding.

7. Agentic AI

Agentic AI is very useful in transaction monitoring and fraud detection in real-time. Agentic AI can autonomously plan and execute a sequence of actions to achieve a specific goal. A key strength of agentic AI is its ability to break down complex problems and adapt its actions based on context and feedback. This is achieved by orchestrating multiple specialized AI "agents" that work together seamlessly, such as a "PEP agent" or "Monitoring agent" or "Payment initiation agent".

7. Quantitative Analysis

An analysis of how to Build better classification, prediction approach for fraud detection and risk assessment by leveraging Quantum Machine Learning

Problem Statement:

Overcome the limitations of Classical machine learning algorithm in classification of Imbalanced Data:

Classical machine learning based predictions and classifications are good but has limitations when It comes to highly imbalanced data. In such scenario they often struggle to have better Precision and Accuracy and could lead to False Positives and False Negatives. We have used Quantum Support Vector Machine algorithm for the Transaction monitoring / Fraud Detection use cases that is based on the classification of labeled data.

Infrastructure: We have executed our Program on IBM Quantum system

Quantum Machine Learning (QML) leverages quantum mechanical phenomena like Superposition and Entanglement, which helps QML models uncover the hidden patterns and correlations between data points of complex, inadequate, and imbalanced data sets.

Solution : We used data-set preprocessing to improve the quality of data for fraud detection.

- To model the data-set we used the Quantum Support Vector Machine (QSVM)
- For encoding classical data into quantum bits ZZ- FeatureMap is used
- Simultaneous Perturbation Stochastic Approximation (SPSA) optimization was used to optimize the hyperparameters for the kernels to achieve highest accuracy.

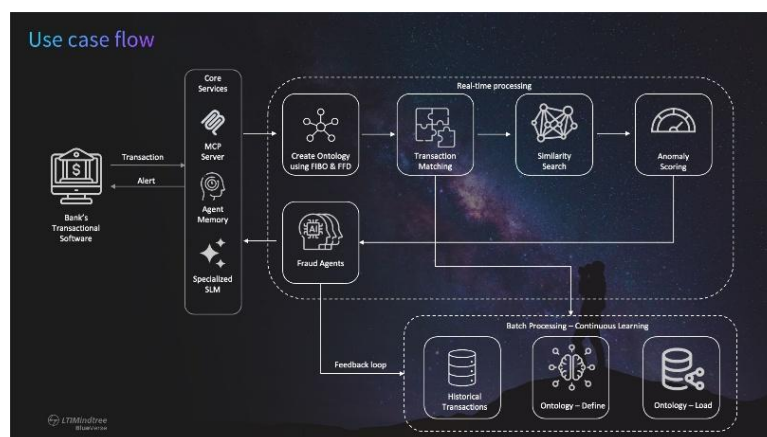
- Quantum kernel is used to compute the kernel matrix which helps in constructing the hyperplane

Higher Prediction Accuracy: Quantum SVM experimentation generated promising results on **IBM Quantum system**, such as improved prediction accuracy in the case of transaction fraud detection benchmarked against Classical SVM.

Classical SVM	Precision	Recall	F1-score	Support
0	0.97	0.997	0.98	479
1	0.86	0.30	0.44	20
Macro avg	0.91	0.65	0.71	499

Quantum SVM	Precision	Recall	F1-score	Support
0	0.98	1.00	0.99	479
1	1.00	0.60	0.75	20
Macro avg	0.99	0.80	0.87	499

An analysis of how to build a next gen fraud management approach using Agentic AI - Agentic AI orchestrates real-time multi-agent detection, using contextual cues, memory, and dynamic reasoning to flag anomalous behaviour as it occurs. It also embeds human-in-the-loop feedback for continuous improvement.



8. Challenges and Risks of AI in Financial Crime Compliance

- **Explainability and Model transparency:** A challenge in this area is that it is highly regulated so explainability and transparency of the models is an imperative. Models using Neural Networks find it a challenge for it to be explainable.
- **Data privacy:** Data privacy poses few distinct challenges. The tenets of data minimization and purpose limitation inhibit the exploratory data analysis from collecting the whole dataset needed to train the model. So we have to implement a robust data governance framework and use a robust privacy enhancing mechanism.
- **Regulatory and compliance challenges:** Supervisors require assurance that AI does not weaken compliance standards.
- **Imbalanced datasets:** The number of fraudulent transactions which occurs to the total number of transactions is very minimal. 1 in 100 or 1 in 1000. The practical strategy is to generate synthetic data to be generated to increase accuracy using Generative Adversarial Networks or to use Quantum Machine Learning in addition to classical flow for better results.
- **Algorithmic Bias-** Algorithmic bias and hallucinations are reduced by having humans in the loop for decision making. This also balances automation with customer trust. AI will aid and abet humans in decision making not replace them.
- **Interoperability between IT Legacy Systems and AI –** One of the technical challenges is interoperability with IT systems and AI and use of tools like MCP and A2A and building interfaces with Legacy systems will help address this challenge.

9. Conclusion

Of all the major technology developments in the last 25 years – Moore’s Law and the personal computer, internet, mobile phones and currently it is AI. AI is neither a saviour which will solve everything nor replace humans.

Financial Crime, Anti-Money Laundering and Fraud Detection is one area where emerging technologies like AI and Machine Learning have a big role to play in improving operational efficiency, risk reduction and cost savings.

There is tremendous potential for use of AI in financial crime in making tasks and life easier which aid and abet humans in their day to day jobs. We must to a large extent have a human in the loop for decision making.

With the advent of increased sophistication in financial crime , fraud investigators can uncover fraud long after the transaction takes place as well as in real-time in some cases.

Real success in AI stems for solving problems in this space requires all entities government , organizations , leaders and society to focus the use of emerging technologies in solving challenges which they are facing.

References

Ahmad Naser Eddin 1, Jacopo Bono 1 et al - Anti-Money Laundering Alert Optimization Using Machine Learning with Graphs

New York City Bar - Artificial Intelligence and Machine Learning in Financial Services – Opportunities and challenges in AML and combatting the financing of terrorism

Faheem Ashraf , Alejandro Schaffer - Combating Financial Crime: AI and Machine Learning in Anomaly Detection and Risk Management

[Digital Payments Intelligence Platform — RBIH](#) – Centralized fraud intel and real-time risk scoring

[MuleHunter.ai — RBIH](#) - Detect and flag mule accounts in near real-time

[Opportunities and Challenges of New Technologies for AML/CFT](#) – FATF
