Checkmate to financial crimes!

April 2022

By Suveer Khanna, Partner, Forensic Services, KPMG in India and Krishna Pandala, Technical Director, Forensic Services, KPMG in India

(6 min read)

Key takeaways:

- *Senior management must forge a strong partnership with the industry ecosystem, including the government, the regulators, and the customers, to uplift the level of financial crime compliance across the industry*
- *Artificial Intelligence models must be closely monitored and carefully adjusted to ensure they continue to perform with precision over time*
- *Establishing effective Machine Learning operational processes to monitor drifts and validate results is critical to perfecting the endgame*

The fight against financial crimes is a continuous challenge for institutions and banks around the world. As financial crime typologies grow more complex and sophisticated, it has become more challenging for financial institutions to keep pace with these new emerging typologies and crime patterns.

Artificial Intelligence (AI) offers capabilities to adapt to new threats, such as new money-laundering schemes and financial crime patterns, thereby ensuring that firms can adapt quickly in different regulatory environments and stay one step ahead of criminals.

However, AI solutions also come with challenges which continue to derail their successful implementation. This can happen due to several factors, such as data unavailability, poor data quality leading to inaccurate predictions and lack of expertise to be able to balance both the compliance needs and technical capabilities in the offer. But for how long can financial institutions afford to delay this and risk losing their reputations in the bargain? It is time to checkmate financial crime offenders with smart solutions.

First move: In chess, the first move is very important as it allows the player to gain control of the centre and strengthen their position. In financial crime, data is at the centre stage of AI projects with the potential to support a variety of use cases, including transaction monitoring, fraud pattern recognition, internal fraud behavioural analytics, alert discounting, customer risk rating and others. However, with disintegrated legacy systems, manual processes and unstructured open-source intelligence, it is difficult for financial institutions to channelise insights from distributed data sets.

Successful stakeholders at various financial institutions have adopted a simple two-pronged strategy to charter their course of maneuvering their first AI project. The first move is to identify a single use case that can create maximum impact and is most scalable across their organisation. The second move is to lay down the tenets of data strategy, which may range from setting up data-pipeline infrastructure to designing an effective operating model to fostering a strong data culture. This strategy manifested into the stakeholders' first move, which included a cohesive strategy with cross-functional teams and a buy-in from senior executives. Getting the first move right is critical towards laying a strong foundation and gaining control of the project.

The middle game: In chess, understanding the concept of a weak square and a strong centre will help in strengthening your defence and preparing for attack. In financial crime, strength-weakness is defined strategically by organisational behaviour and tactically by data integrity. Weakness in any one of these areas will leave weak squares open for attack by financial crime offenders.

A strong organisation culture requires a pervasive approach, ensuring every employee sees fighting financial crime as a core responsibility. Further, the senior management must forge a strong partnership with the industry ecosystem, including the government, the regulators and the customers, to uplift the level of financial crime compliance across the industry. Finally, the second line of defence should be empowered to monitor the first line as they go about building their business.

Such measures would not only strengthen the defence but also take the attack back to the financial crime offenders. One of the key tactical elements of attack is the data. Data is often spread across different disparate systems, inconsistent processes and complex terminology, making it difficult to derive insights for building smart solutions. Organisations must harness data groups that span across different departments for developing financial-crime data lakes that houses sufficient high-quality data for AI models. These initiatives would help develop a strong middle game, laying the groundwork for the endgame.

The endgame: Chess is a zero-sum game that ends with a checkmate. Financial crime is not. In fact, it is the beginning of a continuous battle that must be fought with precision. The challenge is further amplified as AI models degrade over time due to their dynamic nature and sensitivity to market conditions. As a result, AI models must be closely monitored and carefully adjusted to ensure they continue to perform with precision over time.

Establishing effective Machine Learning operational processes to monitor drifts and validate results is critical to perfecting the endgame. Beyond that, the models must have the ability to demonstrate financial crime compliance to regulators, ensure there are no hidden biases in its data sets and adhere to transparency principles so that incorrect decisions can be traced. Such activities with detailed planning is expected to ensure that the endgame is set up to defend financial institutions from being exploited by financial crime offenders.

To conclude, financial systems are the vanguard of preventing financial crime. It is vital to invest time and resources in building smart solutions and protecting one's reputation.