Deloitte.

India Banking Fraud Survey

Edition IV
January 2022

Need to enhance EWS and FRM using AI/ML

The increase in the use of digital channels for transactions by customers, on one hand, has contributed to the ease and speed of transactions. On the other hand, with evolving business models and increased technology use, fraud risk management frameworks have been introduced to newer
and more complex challenges.

This ever-evolving technology across banking channels means that human decision-making and traditional transaction alert systems are no longer effective in the timely detection of frauds.

Digitalisation of business transactions has led to an enormous increase in transactions every day, which in turn, has rapidly increased the volume of bank transaction datasets. Interestingly, this data holds several valuable insights that can identify fraudulent behaviour or patterns in the transaction activities of a particular customer at an early stage. An intelligent data analytics tool can mine through vast volumes of data, gather and analyse intelligence from external sources, and identify hidden relationships and red flags. This will enable banks to proactively identify potential fraudulent transactions before they manifest themselves. Through human decision-making, along with machine learning algorithms (that can learn from these datasets), fraud risk identification and detection can be much faster and more efficient.

Currently, most early-warning and transaction monitoring systems that generate fraud alerts are rule-based. When a certain threshold exceeds/certain conditions are met/recurrence is identified, the transaction is marked for further investigation. One operational challenge of such traditional EWS and fraud alert monitoring systems, with predefined thresholds/ parameters, is the number of "false positives"—transactions that are flagged as suspicious, but that turn out to be regular. Following up and investigating such false positives can be a very time-consuming and cost-intensive activity for banks. However, by performing periodic reviews of test results and incorporating learnings into monitoring systems, the existing system can learn to detect true anomalies more efficiently, with lower false alarm levels.

To obtain better results, AI techniques can be used to reduce false positives and spot true positives and detect new patterns. Anomaly detection algorithms are tailor-made to detect fraudulent transactions by isolating exceptional items based on variables known to the model. The input from risk, compliance, and business teams complemented with intelligence gathered through external sources is essential to implement this use case. In addition, banks can use data segmentation, coupled with statistical analyses to identify characteristics specific to each peer group and create custom thresholds. For example, high net-worth customers tend to be associated with large transaction amounts and may therefore require different parameters than lower income clients. Banks can then perform a sensitivity analysis to help determine whether threshold levels should be increased if too many false alerts are generated or decreased if suspicious activity is being missed, a process known as alert tuning.

There are several benefits to utilising ML in fraud monitoring and detection:

- Works with large datasets – ML is better than humans at processing large datasets and its prediction results improve as datasets grow.
- Reduces operational cost – It eliminates the need to spend as much time and resources on reviewing every alert transaction due to better accuracy and automated predictions.
- Detects and prevents fraud more effectively – ML can quickly adapt to new behaviours of fraudulent transactions and helps improve reactions to suspicious outliers.
- Reduces false positives and prevents frauds with more efficacy.

Advanced analytics can help reshape the way banks conduct fraud tests and monitor their operations. In fact, without using proper data interrogation techniques, efficiently and effectively using all the sources of information available—both internal and external—the process of uncovering fraudulent behaviours may not be as accurate as desired and can take more time and effort, given the large volumes of data generated by banks.

Deloitte.