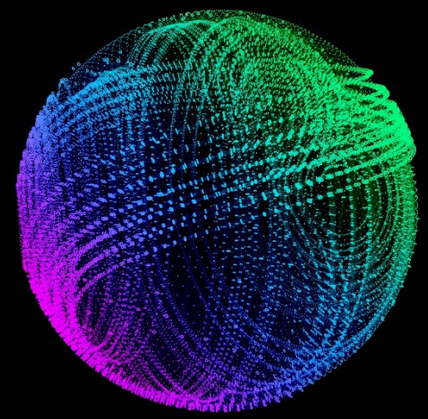
Deloitte.

5x5 series: Insights and actions

Developing and monitoring AI-based payment fraud models



As payment fraud schemes become more complex, and as regulatory agencies share new standards for model risk management, many organizations are building, expanding, and assessing their fraud detection models.

5 insights you should know

1 **Crisis and uncertainty can create opportunities to camouflage malicious intent; therefore, more advanced and adaptable fraud detection techniques may be required to identify emerging schemes**
The COVID-19 pandemic, as well as economic and other societal disruption over the last few years, have created uncertainty in which cyber criminals can exploit to mask their actions. These fraud techniques often include social engineering, malware attack, data breach/mass data compromise, account takeover, identify theft, and collusion. When there are new sources of cash, such as through government assistance programs, this requires additional vigilance and adaptability for new and emerging fraud schemes.

2 **New financial products may require advanced fraud mitigation—without a blueprint of known fraudulent behaviors—warranting support from third-party vendors**
Fraud schemes in the consumer and business payment areas are constantly evolving, and criminals can exploit cyber vulnerabilities—especially during new product launches when controls and fraud detection models may not be mature—to enable fraud. In response, organizations are often working with third-party vendor models and consortium data services, which can collect signals from across multiple organizations, to enable more rapid fraud detection.

3 **New technologies bring new risks to explainability and integration**
As artificial intelligence (AI) is becoming more popular, efficient, and critical to fraud prevention, many risk detection and monitoring models are now AI-based. This brings additional complexities to fraud model owners, who need to explain the results generated by those models and monitor for their accuracy, as well as for technology owners, who are integrating and orchestrating results from these models.

4 **Increasing regulatory interest in AI-driven models means institutions should be prepared for scrutiny**
Banks, FinTechs, and other financial institutions are facing increasing regulatory pressure and scrutiny on establishing sound practices for model risk management. The Office of Comptroller of the Currency (OCC) from US Treasury has issued an updated handbook in August 2021 to advocate model risk management examinations that include areas such as fraud.

5 **Adapting to talent constraints**
To keep pace with AI development, model development and model risk management teams need to have the AI-savvy talent, as well as those familiar with fraud risks and schemes, in order to support the adaptability and scalability of fraud model programs.

5 actions you can take

1 **Integrate risk signals across known fraud, cybersecurity and AML events to identify emerging schemes**
Criminals' dependence on technology leaves a cyber trail that can be exploited to detect, prevent, and disrupt their activities. In order to develop effective fraud detection models, financial institutions can integrate data collected on events across various departments, which often include cybersecurity, anti-money laundering (AML), and fraud groups, as well as risk signals from external consortiums. This often requires the implementation of a centralized data lake to indicate new and emerging fraud schemes.

2 **Leverage vendor models, but manage risks by enhancing your third-party risk management policies**
The widespread use of vendor and other third-party products—including data and models—poses unique challenges for transparency, validation, and other model risk management. Consider updating third-party risk management policies to embed for transparency into model performance.

3 **Use an AI-focused framework for assessing fraud model performance**
An effective model validation framework includes evaluation of model conceptual soundness (e.g., AI training and explainability); model governance (including benchmarks of accuracy and model performance); ongoing monitoring (to confirm model consistently performs within benchmarks); and functional and effectiveness testing (e.g., back testing, threshold tuning, and sensitivity analysis).

4 **Develop frameworks for transparency and regulatory readiness**
Fraud model frameworks should include documentation covering the intended use of the model, including fraud schemes listed in a fraud risk register, and should evidence support of model choices, including modeling approaches, model features, and data selected. Model testing—such as for data completeness, model accuracy and model robustness—should be performed and documented in a form that can be provided to regulatory agencies as needed.

5 **Coordinate teams involved in a fraud model governance framework**
An effective fraud model governance system includes coordination across fraud model owners, fraud model reviewers, independent risk management staff, data ownerships, and representatives from the vendor or model provider. Each team member should have roles and recurring responsibilities that collectively contribute to model governance.

Connect with us

Mike Weil
Managing Director
Deloitte Financial Advisory Services LLP
miweil@deloitte.com

Satish Lalchand
Principal
Deloitte Transactions and Business Analytics LLP
slalchand@deloitte.com