ARTICLE

Navigating the Complexity of Models and Model Validation in Financial Crimes

July 3, 2025 | 2 minutes reading time | By Fenton Aylmer

Fraud detection and anti-money laundering are among the complicated financial crime risks that financial institutions must model. How do these risks differ, what type of modeling do they require, and how can varying models – including AI methodologies – be properly validated?

Today, financial institutions face evolving threats from fraud and sophisticated money laundering activities, and operate under intense regulatory scrutiny. As their reliance on detection models

deepens, so does the complexity of validating these models to ensure operational effectiveness, ethical integrity and regulatory compliance.

Fenton Aylmer, Adjunct Enterprise Risk Management Professor, Columbia University

This article explores critical differences in models and validation frameworks for financial crimes, as well as the emerging role of artificial intelligence (AI) in this area.

Before we discuss challenges and divergences in model validation, it's important to understand how models for fraud and AML differ, particularly with respect to monitoring and risk horizons:

External vs. Internal Threat Monitoring

Fraud models focus on detecting external anomalies (i.e., unauthorized activities originating outside the institution) and require rapid anomaly detection and immediate response.

AML models, in contrast, monitor long-term customer behavior, aiming to detect slow-moving, sophisticated patterns indicative of money laundering activities.

Short-Term vs. Long-Term Risk Horizons

Fraud detection operates on short time scales, with models required to intercept anomalous behavior in real time or near-real time.

AML detection, on the other hand, requires sustained behavioral monitoring over months or years, necessitating models attuned to gradual shifts in transactional patterns.

Validation Challenges

Now that we understand the areas of coverage of fraud and AML models, let's consider their core differences with respect to validation:

Data Availability and Performance Metrics

Fraud models benefit from abundant event data, enabling validation using standard machine-learning metrics – such as precision, recall and F1 scores.

AML validation, in contrast, must cover rare-event challenges – leading to greater reliance on scenario testing, typology alignment and evaluation of true positive rates.

Regulatory Scrutiny and Documentation Expectations

AML models have stringent regulatory documentation requirements, including traceability, scenario justification and auditability standards.

Fraud models, meanwhile, often balance operational performance demands against regulatory expectations, emphasizing detection accuracy and customer service.

Artificial Intelligence: New Capabilities, New Risks

The integration of AI into financial crime detection introduces transformative capabilities but also raises profound validation challenges.

AI systems based on deep learning, for example, often exhibit "black box" characteristics where model decision paths are difficult to interpret. Key challenges in validating AI-enhanced models include: (1) ensuring explainability to satisfy both operational stakeholders and regulatory examiners; (2) identifying and mitigating algorithmic biases that could impact detection fairness; and (3) designing governance frameworks capable of balancing operational efficiency with ethical assurance.

When evaluating AI-driven models, validators must incorporate interpretability methods and ethical risk assessments, in addition to traditional statistical techniques.

Parting Thoughts: Communication and Continuous Evolution

The ability to bridge communication gaps across technical, business and regulatory teams is one of the keys to model validation effectiveness. Effective validation frameworks recognize that, beyond statistical rigor, there must be a shared understanding of model purpose, risk thresholds and compliance obligations.

Cross-disciplinary fluency — translating model behaviors into business impacts and regulatory defensibility — is another critical competency for modern validation teams.

It is important to keep in mind that financial crime detection is a continuously moving target, shaped by both regulatory developments and innovation, which is sometimes adversarial. Model validation must evolve accordingly, blending technical mastery with adaptability, ethical vigilance and regulatory intelligence.

Successful validators integrate technological advancements with responsible risk governance at every stage of model lifecycle management.

Fenton Aylmer *is a strategist and risk expert with over 30 years of experience advising boards and C-Suite executives in financial services and FinTech. He most recently led product development and partnerships at Entelligent, a climate risk analytics firm, and teaches enterprise risk management at Columbia University. Fenton's career spans senior roles at New York Community*

Bank, Citigroup, EY, KPMG, and Bank of Montreal, with deep expertise across enterprise, operational, conduct and regulatory capital risk.

*This article was based on a recent guest lecture at Columbia University by **Chandrakant Maheshwari**, a modeling expert with more than two decades worth of experience in data analytics, validation and financial crime risk management.*

Topics: **Model Risk**

SHARE

Related Insights

ARTICLE

Built In, Not Bolted On: AI Risk Management Belongs in the Architecture

JULY 2

Regulators are evaluating artificial intelligence based on its domain,...

Model Risk, **Data & AI Model Governance**

Read Article

ARTICLE Members Only

Anthropic's Mythos: Frontier AI Shakes Up Cybersecurity and Regulation

JULY 2

A select group of corporations gets early access to powerful agentic s...

Cybersecurity, **Regulation & Compliance**, **Model Risk**, **Data & AI Model Governance**

Read Article

ARTICLE

Markets Are Underestimating Risk in a Fast, Fragile World