Model Governance Documentation

* * *

Bank Account Fraud Detection

Last update: 12 February 2026

Version number: 1.0

Status: In Progress (unpublished)

1. Overview

1.1 Purpose of the Document

Model Risk Management (MRM) is a critical aspect of any financial institution, especially those dealing with fraud detection.

Bank Account Fraud (BAF) Detection aims to develop and implement a mix of models to identify fraudulent bank accounts. This documentation aims to meet Supervisory Letter SR 11-7 standards.

Supervisory Letter SR 11-7

SR 11-7 is a set of standards and guidelines developed by the United States Securities and Exchange Commission (SEC) to ensure that financial institutions have robust systems in place for detecting, preventing, and responding to fraud. Essential components of SR 11-7 include:

- **Definition of a Model**: Any quantitative method, system, or approach using statistical or economic theories to process data into estimates.
- **Model Validation**: An independent, comprehensive review to ensure models are accurate and appropriate for their intended use.
- **Governance and Controls**: Banks must establish strong policies, procedures, and accountability mechanisms for model development, implementation, and ongoing monitoring.
- **Scope**: Applies to all institutions supervised by the Federal Reserve or OCC, including national and state banks.

Documentation Components

1 Model Identification and Purpose

   a. **Model Name and Version**: Unique identifiers that track the specific iteration of the fraud model being deployed.

   b. **Business Use Case**: A clear statement defining how the model detects specific fraud typologies within the BAF dataset, such as account takeover or synthetic identity fraud.

   c. **Model Owner and Stakeholders**: Documentation of the individuals or teams accountable for the model's performance and regulatory compliance.

2 Data Integrity and Lineage

   a. **Data Sources and Scope**: A description of the input variables from the BAF dataset, including transaction attributes and behavioral features.

b. **Data Quality Assessment**: Evidence of checks for missing values, outliers, and data freshness to ensure the model isn't learning from "garbage" data.

c. **Feature Engineering Rationale**: An explanation of why specific derived features were created to capture complex fraud patterns.

3 Model Development and Methodology

a. **Algorithm Selection**: Justification for choosing specific architectures (e.g., Random Forest vs. Neural Networks) based on the BAF dataset's characteristics.

b. **Model Assumptions and Limitations**: A transparent list of what the model cannot do and the conditions under which it might fail.

c. **Training and Testing Split**: Details on how the data was partitioned to prevent data leakage and ensure the model generalizes well to unseen fraud.

4 Validation and Testing

a. **Performance Metrics**: Results of testing using metrics like Precision, Recall, and the Area Under the Precision-Recall Curve (AUPRC), which are critical for imbalanced fraud data.

b. **Sensitivity Analysis**: Documentation of how the model reacts to changes in input variables or shifts in fraudster behavior.

c. **Backtesting Results**: A comparison of predicted fraud vs. actual historical outcomes within the BAF suite to prove accuracy.

5 Implementation and Monitoring

a. **Deployment Environment**: A description of the technical infrastructure where the model resides and how it integrates with real-time payment rails.

b. **Ongoing Monitoring Plan**: The schedule and thresholds for tracking "model drift" to ensure the model stays effective as fraud tactics evolve.

c. **Change Management Process**: A formal protocol for how the model will be updated, retrained, or decommissioned in the future.

1.2 Document Version Control

Document version	Change date	Approver	Status
1.0	12 February 2026	George Li	Approved

2. Model Identification and Purpose

2.1 Model Name and Version

2.2 Business Use Case

2.3 Model Owner and Stakeholders

3. Data Integrity and Lineage

3.1 Data Sources and Scope

3.2 Data Quality Assessment

3.3 Feature Engineering Rationale

4. Model Development and Methodology

4.1 Algorithm Selection

4.2 Model Assumptions and Limitations

4.3 Training and Testing Split

5. Validation and Testing

5.1 Performance Metrics

5.2 Sensitivity Analysis

5.3 Backtesting Results

6. Implementation and Monitoring

6.1 Deployment Environment

6.2 Ongoing Monitoring Plan

6.3 Change Management Process