**Y:\BSA_OFFICE_SECURED\Policy and Procedures\Templates\Logo\Screen - EWB English Logo - small.png**

**Alipay**

**Digital Banking**

**February/2025**

**Model Documentation Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Author** | **Reviewer** | **Date** | **Details of the Changes** |
| EWB |  | 2-14-2025 | Initial draft report created |
| EWB |  | 2-20-2025 | Revision and updates |
| EWB |  | 2-28-2025 | Minor Edits |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. EXECUTIVE SUMMARY 5](#_Toc191977158)

[1.1 Objective and Background 5](#_Toc191977160)

[1.2 Model Purpose & Use 6](#_Toc191977161)

[1.2.1 Model Purpose 6](#_Toc191977162)

[1.2.2 Portfolio/Product/Transactions Overview 7](#_Toc191977163)

[1.2.3 Applicable Policies and Regulations 8](#_Toc191977164)

[1.2.4 Existing Models 8](#_Toc191977165)

[1.2.5 Upstream/Downstream Model Dependencies 8](#_Toc191977166)

[1.2.6 Process Flow Diagram 9](#_Toc191977167)

[1.3 Model Key Stakeholders, Change Management, & Outstanding Issues 10](#_Toc191977168)

[2 INPUT DATA INTEGRITY & APPROPRIATENESS 10](#_Toc191977169)

[2.1 MODEL DEVELOPMENT DATA 10](#_Toc191977170)

[2.1.1 Overview of Model Development Data 12](#_Toc191977171)

[2.1.2 Development Data Sources, Extraction Process, and Reconciliation 13](#_Toc191977172)

[2.1.3 Development Data Preparation 15](#_Toc191977173)

[2.1.4 Data Limitations 19](#_Toc191977174)

[2.1.5 Data Preparation Software / Platform 19](#_Toc191977175)

[2.1.6 Data Retention 19](#_Toc191977176)

[3 CONCEPTUAL SOUNDNESS 20](#_Toc191977177)

[3.1 MODEL THEORY AND ASSUMPTIONS 20](#_Toc191977178)

[3.1.1 Model Theory and Methodology 21](#_Toc191977179)

[3.1.2 Segmentation Approach 24](#_Toc191977180)

[3.1.3 Model Settings 24](#_Toc191977181)

[3.1.4 Model Assumptions 25](#_Toc191977182)

[3.1.5 Model Limitations and Weaknesses 25](#_Toc191977183)

[3.2 MODEL ESTIMATION / TRAINING AND SELECTION 27](#_Toc191977184)

[3.2.1 Estimation Methodology and Assumptions 27](#_Toc191977185)

[3.2.2 Modeling Software / Platform 28](#_Toc191977186)

[3.2.3 Hyper-parameter Tuning 28](#_Toc191977187)

[3.2.4 Feature / Variable Selection 29](#_Toc191977188)

[3.2.5 Model Estimation / Training Results 30](#_Toc191977189)

[3.2.6 Other Types of Model Estimation 31](#_Toc191977190)

[3.3 Model Development Testing 32](#_Toc191977191)

[3.3.1 Statistical and Technical Assumptions Testing 33](#_Toc191977192)

[3.3.2 Model Performance / Fit Testing 33](#_Toc191977193)

[3.3.3 Model Stability and Overfitting Testing 35](#_Toc191977194)

[3.3.4 Back-testing 35](#_Toc191977195)

[3.3.5 Model Explainability Testing 37](#_Toc191977196)

[3.3.6 Benchmarking 38](#_Toc191977197)

[3.3.7 Sensitivity Analysis 39](#_Toc191977198)

[3.3.8 Stress Testing / Scenario Analysis 39](#_Toc191977199)

[3.3.9 Other Testing 40](#_Toc191977200)

[3.3.10 Overall Performance Assessment 40](#_Toc191977201)

[3.3.11 Need for Model Overlays 41](#_Toc191977202)

[4 PRODUCTION PROCESS COMPLETENESS & ACCURACY 41](#_Toc191977203)

[4.1 Production Application Testing 42](#_Toc191977204)

[4.1.1 System Testing Approach and Results 42](#_Toc191977205)

[4.1.2 User Acceptance Testing Approach and Results 43](#_Toc191977206)

[4.2 Model Production Specifications 43](#_Toc191977207)

[4.2.1 Model Platform 43](#_Toc191977208)

[4.2.2 Data and Process Flow Diagram 44](#_Toc191977209)

[4.2.3 Input Data Specifications 44](#_Toc191977210)

[4.2.4 Model Formulas / Algorithms 46](#_Toc191977211)

[4.2.5 Model Parameters and Settings Values 46](#_Toc191977212)

[4.2.6 Model Outputs 47](#_Toc191977213)

[4.2.7 Reports 47](#_Toc191977214)

[4.3 Operational Controls 47](#_Toc191977215)

[4.3.1 Model Access and Security 48](#_Toc191977216)

[4.3.2 Production Deployment 48](#_Toc191977217)

[4.3.3 Model Usage Controls 49](#_Toc191977218)

[4.3.4 Model Backup 49](#_Toc191977219)

[4.4 Contingency Plans 50](#_Toc191977220)

[4.4.1 Disaster Recovery Plan 50](#_Toc191977221)

[4.4.2 Business Continuity Plan 51](#_Toc191977222)

[4.5 Operating Procedures / User’s Guide 51](#_Toc191977223)

[5 ONGOING MODEL GOVERNANCE & OUTCOME ANALYSIS 53](#_Toc191977224)

[5.1 Ongoing Risk & Performance Monitoring Plan 53](#_Toc191977225)

[5.2 Model Approval and Change Management Process 56](#_Toc191977226)

[5.2.1 Model Approval Process 56](#_Toc191977227)

[5.2.2 Model Change Log 56](#_Toc191977228)

[6 APPENDICES 57](#_Toc191977229)

[6.1 Appendix A 57](#_Toc191977230)

[6.2 Appendix B 57](#_Toc191977231)

# EXECUTIVE SUMMARY



## Objective and Background

Please provide a high-level description of:

* The model’s business objectives.
* Business background including history where appropriate.
* Related regulatory requirements that relate to the business objectives.
* Any other information you see appropriate.

Model Owner: The Alipay Fraud Model is a rule-based fraud detection system used by East West Bank (EWB) for global remittance transactions processed through World First Asia Pvt Ltd. The model’s primary objective is to evaluate and mitigate fraud risks associated with global remittance transactions on the Alipay platform. By leveraging predefined risk rules, the model assesses transactions in real time, ensuring compliance with risk management policies while minimizing fraudulent activities.

Alipay was introduced by Digital Bank in 2020. Alipay conducts transfers from EWB to accounts in mainland China and provides real time foreign exchange rate from US Dollar (USD) to Chinese Yuan (CNY) also known as renminbi (RMB). The account holder must be a Chinese national. Accepted remittance for goods payments, service payments, home remittance and salary.

When an Alipay transfer is processed, the model evaluates input data against established fraud detection rules. If a mismatch exceeds the preset risk appetite, the transaction is suspended for manual review. This approach enhances the security and integrity of cross-border remittances while allowing legitimate transactions to proceed smoothly.

Alipay, operated by Ant Group, is a leading digital payments and financial services platform, widely used for e-commerce, peer-to-peer (P2P) payments, and global remittance transactions. In partnership with East West Bank, the platform facilitates seamless cross-border money transfers, ensuring compliance with financial regulations while mitigating fraud risks.

World First Asia Pvt Ltd, a global payments service provider, supports global remittance services for Alipay. Given the increasing sophistication of fraud schemes targeting digital transactions, the need for a robust fraud detection framework has become essential. The Alipay Fraud Model is designed to strengthen transaction monitoring and enhance fraud prevention strategies in response to evolving financial crime threats.

|  |  |
| --- | --- |
| **Model Name** | * *Please provide the official model-name that is used by the model owners and the MRM Group (mutually agreed).*   Model Owner: Alipay Fraud (Model ID: 059) |
| **Primary Model Owner Entity** | * *Please provide the model owner business entity name, e.g., US, China, or Hong Kong.*   Model Owner: US |
| **Primary Model Owner Group** | * *Please provide the model owner business group name.*   Model Owner: Enterprise Risk Management (Ant Group) |
| **Model Owner** | * *Please provide the model owner names.*   Model Owner: FVP – ERM Data Manager |
| **Model Developer** | * *Please provide the model developer names (vendor name if vendor model).*   Model Owner: Alipay <https://www.alipay.com/> |
| **Model Production Process** | * *Please provide the model production process environment. A high-level description is encouraged.*   Model Owner: Ant Group maintains technical fraud detection platform powered predominantly by local regulator rules. This platform uses a very large dataset of the data points available regarding the customers, their transactions, and any other relevant information. The Platform is built and maintained by the vendor’s internal Fraud detection team, who ensure the stability and improvement of all these workings. |
| **Model User** | * *Please provide all model usernames along with business group names.*   Model Owner: Digital Banking |
| **Portfolios the Model Applies to** | * *Please provide high level portfolio size and description that the model is applied to.*   Model Owner: Alipay applies to all Digital Banking customers. |
| **Model Objective** | * *Please list all model objectives at a high level.*   Model Owner: The Digital Bank offers customers the ability to send Alipay transactions, which are similar to P2P (person to person, like Zelle) transactions. It allows customers to make transactions using either a phone number or email address as tokens (again - very similar to Zelle). Ant Group maintains a fraud detection platform that interrogate Alipay transactions. |

## Model Purpose & Use

### Model Purpose

For each business purpose, discuss the following in detail:

* The overall business purposes.
* The specific role that the model output plays in business use (for example, if the model output is used as a secondary source of information in the decision-making process, this should be detailed here).
* The specific products/portfolios/customers/transactions for which the model is suitable (e.g., types of retail mortgages, types of derivatives, types of consumer transactions, etc.)
* Any restrictions on model use, for example, excluded product types within product categories or transaction size limits.

Model Owner:

The Alipay Fraud Model is a rule-based fraud detection system designed to evaluate and mitigate fraud risks associated with global remittance transactions processed through East West Bank (EWB) via World First Asia Pvt Ltd. The primary purpose of the model is to enhance transaction security by identifying and suspending potentially fraudulent remittance activities before they are processed. This supports EWB’s commitment to financial crime prevention, regulatory compliance, and the protection of customers from unauthorized transactions.

The model aligns with EWB’s broader fraud risk management strategy by ensuring that high-risk transactions are subject to additional scrutiny. By leveraging predefined fraud detection rules, the model enables real-time monitoring and intervention to prevent financial losses, regulatory breaches, and reputational damage.

The output of the Alipay Model serves as a primary fraud detection mechanism within EWB’s global remittance operations. When a transaction is initiated, the model assesses various risk factors, comparing transaction attributes against predefined rules and thresholds. If a mismatch exceeds the established risk appetite, the transaction is flagged for manual review by the fraud operations team before further processing.

### Portfolio/Product/Transactions Overview

* Provide the current size of the portfolio of assets or liabilities (if applicable) and describe the history of the portfolio characteristics (e.g., the inception time frame, any notable idiosyncratic events such as mergers/acquisitions or asset sales, any notable management strategic changes, etc.)
* If the model is being applied to analyze transactions or events (e.g., debit card transactions analyzed for money laundering risk, or cyber-attacks on the Company’s infrastructure), provide the historical volumes of transactions and trends.
* Describe any specific product/customer/transaction types that are being proxied by other product types (e.g., a new product for which the model developed on a more seasoned product is applied).
* When applicable, please describe which portion of the portfolios/transactions/products that is supposed to be covered by the model (for the same business objective) but is decided to be excluded. For such portion, what business strategies are applied to ensure the same business objective is met (e.g., for BSA/AML purpose, certain transactions are monitored manually instead of using the BSA/AML model).

Model Owner:

The bank offers Alipay, a real-time foreign exchange transfer remittance process available to customers enrolled in Digital Banking. As of March 31, 2024, there were 242,387 active customers using Digital Banking, with an aggregate deposit account portfolio balance of $15,113,592,594.

The aggregate portfolio balance is greater than 5% of the total assets $70.876 billion as of March 31, 2024, based on the published EWBC 1Q 2024 earnings release.

### Applicable Policies and Regulations

* List and discuss all regulatory, accounting, legal, and/or compliance rules that are relevant to the model data, design, or use (if any).
* List and discuss all applicable internal policies relevant to the model design and use, if any.

*Note: Please provide document name including suffix.*

Model Owner:

**Regulatory Requirements**

The Alipay Fraud Model operates within the regulatory framework governing global remittance and fraud prevention. While the vendor has indicated that all policies are confidential and for internal use only, the model aligns with China’s Anti-Money Laundering (AML) law and foreign financial regulatory authorities. As Ant Group does not offer cash withdrawal and cash advancement services, financial regulatory institutions do not regulate Alipay as a full-fledged online virtual bank.

By adhering to best practices, the Alipay model supports fraud risk mitigation while maintaining compliance with financial crime prevention standards.

### Existing Models

* If this model is replacing existing model(s), provide details of the existing model(s) and the rationale for the replacement.
* Discuss whether the existing model(s) will be retired once this model goes into production.

Model Owner:

Not Applicable. There are no plans to retire the existing model, as this rule-based approach complements Alipay’s overall fraud detection strategy, allowing the system to adapt to emerging fraud risks effectively.

### Upstream/Downstream Model Dependencies

* Provide a listing and description of upstream and/or downstream models or other key systems (e.g., the Empyrean ALM model).
* Discuss the impact of known limitations of upstream models on this model.

Model Owner:

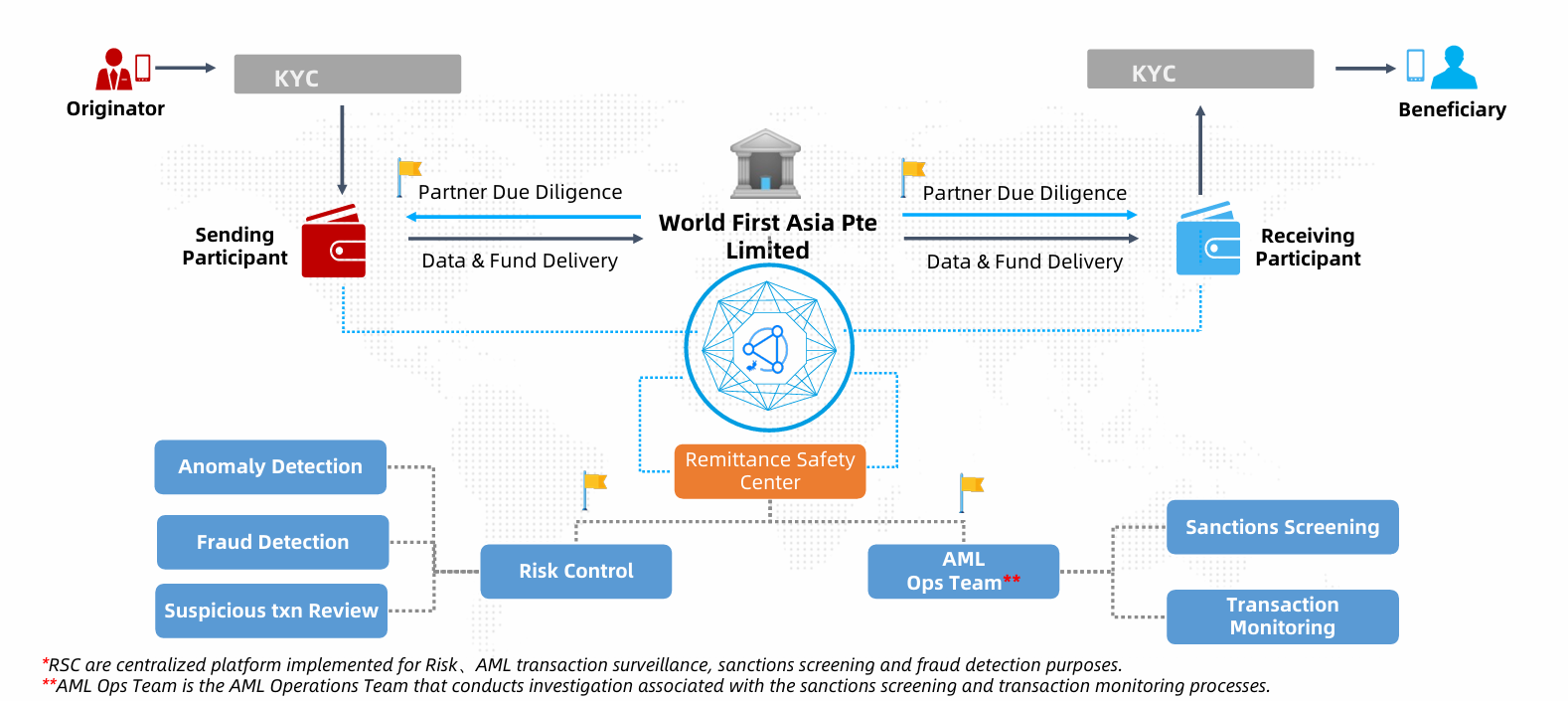
Not Applicable. The Alipay fraud detection model operates independently, without direct upstream or downstream dependencies on other models. It functions as a standalone rule-based system within Alipay’s broader fraud prevention framework.

### Process Flow Diagram

* Provide a process flow diagram showing how the model is used by the functional / business area. Include upstream and downstream models and systems listed in Section 1.2.5 Upstream/Downstream Model Dependencies.

Model Owner:

Below is the process flow diagram that outlines the Remittance Safety Center (RSC) and the Global Remittance Risk Management System operated by Ant Group.



The Alipay fraud detection model follows a structured process to assess and mitigate fraud risks in global remittance transactions. Below is a high-level overview of the model’s process flow:

1. **Transaction Initiation** – User submits a remittance request.
2. **Data Collection** – Transaction details are captured.
3. **Fraud Rule Evaluation** – Predefined fraud rules assess risk.
4. **Risk Decisioning** –

* ✅ If *Non-Suspicious*, transaction is approved.
* 🚩 If *Suspicious*, flagged for manual review.

1. **Manual Review (If flagged)** – Fraud team evaluates flagged transactions.
2. **Final Decision and Processing** – The transaction is either processed or declined based on the fraud assessment outcome.

Since the model operates independently, there are no direct upstream or downstream dependencies on other models. However, it interacts with Alipay’s broader fraud prevention framework, leveraging real-time monitoring and transaction data from the Digital Banking environment.

## Model Key Stakeholders, Change Management, & Outstanding Issues

Describe, at minimum, the following:

1. Model output key stakeholders, review committee(s).
2. High level summary of model changes in recent time or since last model validation.
3. High level summary of the latest model related business area audit and regulatory exam results including any outstanding findings, regulatory Matter Requiring Attention (MRAs), and management self-identified issues.

Please ensure that **all of** the points mentioned above are addressed.

Model Owner:

Alipay is a managed solution and responsible for the fraud detection for both mobile and online payment.

Model Owner is designated to Enterprise Risk Management (ERM), which coordinates with Fraud Strategy Team.

Other key stakeholders of the Alipay fraud detection model are the Fraud Strategy Team, and Digital Banking Operations team. This model has gone through MRM control process including inherent risk assessment.

From January 2025 discussion with Ant Group Management Team, this rule-based model continues to operate based on predefined fraud detection rules, ensuring consistency in its application.

This model is on the pipeline for future model validation.

# INPUT DATA INTEGRITY & APPROPRIATENESS

## MODEL DEVELOPMENT DATA

Model Development Data refers to the data used in the research & development process to determine the model specifications. That is, the process for determining the exact mathematical formulas, algorithms, inputs, parameters, and assumptions that comprise a model.

Note: This documentation section is not applicable for those models whose structure is not determined through empirical data analysis. This includes, for example, some market risk / trading models where the model structure is based on financial theory (e.g., Black-Scholes options pricing model) or qualitative models whose structure and parameters were determined judgmentally.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |

**Data Assumptions Summary**

Please list out data assumptions applied in the model development and model production process, such as missing value treatment, outlier treatment, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Assumption Name** | **Assumption Description** | **Materiality of Assumption** | **Rationales for this Assumption**  (Business driven or quantitative methodology driven) |
| 1 | Missing Data Treatment | If certain input fields are missing, the rule-based model proceeds with available data without imputation. | Moderate | Sourced from discussion with Ant Group Management Team (Global Remittance, Risk Management, Risk Model and AML Officer) – The model operates based on predefined rules, and missing data does not halt processing but may impact rule evaluations. |
| 2 | Rule Evaluation Logic | Transactions are evaluated based on predefined fraud detection rules; no probabilistic scoring is applied. | High | Sourced from discussion with Ant Group Management Team (Global Remittance, Risk Management, Risk Model and AML Officer) – The system relies on rule-based decisions rather than predictive modeling. |
| 3 | Manual Review Process | Transactions that do not meet approval criteria are flagged for manual review. | High | Sourced from discussion with Ant Group Management Team (Global Remittance, Risk Management, Risk Model and AML Officer) – Ensures that high-risk transactions receive additional scrutiny by the fraud detection team. |
| 4 | Data Freshness | The model relies on real-time transaction data for fraud assessment. | High | Sourced from discussion with Ant Group Management Team (Global Remittance, Risk Management, Risk Model and AML Officer) – Real-time data processing is necessary for effective fraud detection. |

**Data Limitation Summary**

Please list out data limitations, their impact of business use, and ongoing monitoring program to appropriately manage the related risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Limitation Name** | **Limitation Description** | **Impact on Business Use** | **Monitoring Description & Frequency** |
| 1 | Outliers Handling | The model does not adjust or remove outliers in transaction amounts, considering them as valid data points for fraud detection. | It is potential to flag legitimate high-value transactions as fraudulent or miss subtle fraud indicators. | Performance checks include periodic reviews of transaction data for outliers, performance checks. along with an assessment of key metrics like detection rate and false positive rate to evaluate the effectiveness. |
| 2 | Historical Data dependency | The model depends heavily on historical transaction patterns to detect fraud, without considering future fraud trends or real-time risk adjustments. | May fail to identify new, evolving fraud schemes that do not align with past patterns. | Fraud trend analysis through manual review volume and rejection rates, with regular historical data updates for ongoing monitoring. |
| 3 | Vendor Data Processing Rules | The vendor’s transaction data processing rules are proprietary and not fully disclosed. | Limited transparency may create challenges in interpreting model outputs. | Gray testing is conducted to align processing rules with fraud detection requirements. |

### Overview of Model Development Data

Provide descriptive characteristics of the model development data, for example, coverage of products / portfolios / transactions, time periods, geographic distribution, etc.

The sources and flows of all the data leveraged in model development should be illustrated with a data flow diagram. The diagram should show each stage of the data preparation process from the initial data pull to the final datasets used for model development and testing including data quality assurance controls.

Model Owner:

The Alipay fraud detection model is a rule-based system that evaluates the risk of global remittance transactions to mainland China. Unlike data-driven models, this system primarily relies on predefined rules and thresholds based on expert knowledge and historical patterns, rather than continuously using historical data to train or update the fraud detection rules.

The model relies on real-time transaction data, including user-provided details such as sender and recipient information, transaction amount, transfer method detail, and other relevant transaction payload from the Digital Banking environment. This data is processed and compared against predefined fraud rules to assess the likelihood of fraudulent activity.

Since the model does not use training datasets in the same way as machine learning models, its development is focused on continuously refining the rules and ensuring AML compliance standards rather than on dataset-driven model improvements.

### Development Data Sources, Extraction Process, and Reconciliation

#### Data Sources

Identify the sources of the model development data, for example, internal data from specific corporate data warehouse tables, desktop databases, text files, or external data from third-party vendors or websites. Development data may also include the output of other upstream models or computational tools.

If both internal and external data are used in the model development, you may want to create subsections covering them separately.

Model Owner:

The Alipay fraud detection model operates using real-time transaction data sourced from the Digital Banking environment. It does not rely on historical development data, as it is a rule-based system rather than a machine learning model.

The primary data sources include:

* **Internal Data:** Transaction details captured through East West Bank’s (EWB) Digital Banking platforms, including sender and recipient information, transaction amount, payment method, and device details.



* **External Data:** Information from third-party vendors, regulatory watchlists, and payment networks to validate transaction authenticity and assess fraud risk.

Since the model does not depend on upstream models or computational tools for data processing, its fraud detection rules are directly applied to incoming transaction data in real-time.

#### Data Relevance

Discuss the relevance of the development data to the modeling objective. For example, is the composition of the development data representative of the current portfolio in terms of coverage and distribution of data attributes? Is the time period selected for development data appropriate for the model’s business purpose and the statistical estimation technique?

If proxies for internal data are used, such as internal data for other products or external data from public databases or third-party services, justify and document the applicability and appropriateness of the proxy data to the specific internal portfolio / purpose.

For vendor models, document a comprehensive assessment of the vendor’s development data applicability to the Company’s internal portfolio/products/customers. This typically involves a comparison of the external and internal data for key model drivers (e.g., geographic distribution, loan/transaction size, loan/product type, etc.).

Model Owner:

As a rule-based model, the Alipay fraud detection system does not rely on historical development data for statistical estimation or model training. Instead, it applies predefined fraud detection rules to real-time transaction data. The data used is directly relevant to the model’s objective of identifying and mitigating fraud risks in global remittance transactions.

The transaction data processed by the model is representative of the current portfolio, as it reflects real-time activities within East West Bank’s (EWB) Digital Banking environment. The data includes sender and recipient details, transaction amounts, payment methods, and device information, ensuring comprehensive fraud risk assessment.

Since this is a vendor-provided model, the fraud detection rules are designed based on industry’s best practices, regulatory requirements, and observed fraud patterns. The vendor ensures that the rule logic aligns with evolving fraud trends and regulatory expectations, making the data applicability consistent with EWB’s remittance transactions. No proxy data or alternative sources are used, as the model directly evaluates transaction-level inputs at the time of processing.

#### Data Extraction Process

Describe how the development data is extracted, either automatically or manually, or otherwise obtained.

Include references to the code or files used to extract the data or to the data files received from other individuals / departments.

Model Owner:

The Alipay fraud detection model operates in real-time and does not require a traditional data extraction process for model development, as it is a rule-based system rather than a data-driven statistical model.

Transaction data is automatically captured from East West Bank’s (EWB) Digital Banking environment at the time of processing. The system collects key transaction attributes, including sender and recipient details, transaction amount, payment method, and device information. This data is then evaluated against predefined fraud detection rules without the need for manual intervention.

Additionally, external data sources such as regulatory watchlists and payment network verifications may be accessed in real-time to support risk assessments. Since the model does not involve periodic data extraction for development, no historical datasets or batch data processing are required.

#### Data Reconciliation

Demonstrate that the development data has been reconciled with a source system (e.g., the general ledger) or line of business report, or alternatively, explain how the extracted data was determined to be complete and accurate.

In addition, provide a step-by-step waterfall of data counts and balances at every step in the data preparation process from the raw data extract to the final modeling dataset.

Model Owner:

As a rule-based fraud detection model, the Alipay system processes real-time transaction data without relying on historical development datasets. Therefore, traditional data reconciliation with a general ledger or line of business reports is not applicable.

To ensure the accuracy and completeness of transaction data, the model directly ingests information from East West Bank’s (EWB) Digital Banking environment. The system continuously validates incoming transaction data by cross-referencing it with payment network records, regulatory watchlists, and internal fraud monitoring systems. Any discrepancies or missing data elements trigger alerts for further review.

Since the model operates in real-time, there is no step-by-step waterfall of data counts from extraction to a final modeling dataset. Instead, transaction data is instantly processed through fraud detection rules, and any flagged transactions are subject to manual review. The effectiveness of the model is assessed through monitoring reports, which track transaction volumes, fraud detection rates, and false positives to ensure ongoing accuracy and reliability.

### Development Data Preparation

#### Data Quality and Treatments

Describe the raw data quality and any treatments used to address missing or erroneous values, for example, algorithms applied to impute values.

Document any analysis of data outliers and their impact on model development / outputs. Provide support for the selected approach for treating the outliers (if any).

Model Owner:

The Alipay fraud detection model processes real-time transaction data and applies predefined rule-based logic to assess fraud risk. Since this is not a statistical or machine-learning model, there is no need for traditional data preparation techniques such as imputation or outlier treatment.

To ensure data quality, the model relies on built-in validation checks within East West Bank’s (EWB) Digital Banking environment. These checks verify the completeness and consistency of transaction data, including sender and recipient details, transaction amount, payment method, and device information. Any missing or erroneous values trigger automated alerts, prompting additional verification before a transaction is processed.

Outlier detection is inherent in the fraud detection rules, which flag transactions exhibiting unusual patterns, such as abnormally high transfer amounts, rapid successive transactions, or deviations from typical user behavior. Since the model is designed to identify anomalies as potential fraud risks, no additional statistical outlier treatment is required. Instead, flagged transactions undergo manual review to determine their legitimacy, ensuring that genuine transactions are not unnecessarily blocked.

#### Data Filtering and Exclusions

Provide a detailed description of, and justification for, data filtering and significant data exclusions that may potentially introduce model bias. Where a significant number of records is excluded due to data quality or other reasons, to the extent possible, analysis should be performed and documented showing the impact of the filtering rule.

A complete waterfall from the point of raw data extract to the final development/testing data showing the impacts of each exclusion (in terms of the number of records and other key metrics) should be provided.

Model Owner:

As a rule-based fraud detection model, the Alipay system does not rely on traditional data filtering or exclusions associated with statistical model development. Instead, the model processes real-time transaction data using predefined rules to assess fraud risk. Transactions with incomplete or unverifiable customer information, those failing regulatory compliance checks (such as sanctions screening), or high-risk transactions exceeding preset thresholds are vetted through AML transaction surveillance, sanctions screening and fraud detection.

Since the model does not generate a structured development or testing dataset, a traditional data waterfall analysis showing record exclusions at various stages is not applicable. However, ongoing monitoring reports track excluded transactions, categorizing them by reason (e.g., failed identity verification, suspicious transaction patterns) to assess the model’s impact on fraud detection and operational efficiency.

#### Data Sampling

Provide details of statistical sampling, if any, performed to create the model development and testing datasets.

Model Owner:

The Alipay fraud detection model does not use statistical sampling to create development or testing datasets. As a rule-based system, it processes real-time transaction data in its entirety rather than relying on sample subsets. The model applies predefined fraud detection rules to all transactions without the need for data sampling techniques typically used in statistical or machine learning models.

Since the model operates on a continuous basis, transaction data is assessed in real time, ensuring full coverage without the need for representative sampling or partitioning into development and testing datasets.

#### Data Transformations

Provide a description of, and rationale for, operations/calculations on raw data, such as scaling, forming data segments, averaging, or combining data from multiples sources (for example, to calculate charge-off rates) in order to produce model development-ready data.

Describe the composite/derived variables created out of raw data. For example, splines, Weight-of-Evidence transformations of variables, interaction terms, etc. Provide support for the technical soundness and appropriateness of the selected transformations in the context of the specific modeling approach you selected and the overall model purpose.

Specifically:

For models that utilize feature engineering, provide detailed documentation of the engineering process, including a description of the software/package used to perform the feature engineering and a discussion on the limitations of the selected engineering approach.

For models that utilize unstructured data, include detailed description of the data pre-processing of unstructured data. Provide analysis/test/comparison results with related data/scripts/outputs if any to justify the pre-processing performed.

For advanced machine learning models, also include detailed discussion on the sufficiency and appropriateness of data transformations and treatments applied with respect to the ML algorithm used (for example, standardization/normalization is required for KNN but not for Random Forests). Provide analysis/test/comparison results with related data/scripts/outputs if any to support the discussion.

Model Owner:

The Alipay fraud detection model is a rule-based system and does not employ data transformations commonly associated with statistical or machine learning models. The model operates on raw transaction data and applies predefined fraud detection rules without modifications such as scaling, segmentation, or feature engineering.

The model does not generate composite or derived variables through transformations like Weight-of-Evidence encoding, interaction terms, or splines. Instead, it evaluates transactional attributes in their original form, assessing risk based on predefined criteria aligned with fraud detection objectives. Since the model does not utilize unstructured data or advanced machine learning techniques, no specialized data preprocessing, feature engineering, or normalization procedures are required.

#### Variable Definitions

Provide definitions of variables, including alternative transformations of variables tested. For vendor models, describe how the vendor’s definitions for inputs and outputs compare with the Bank’s internal definitions (e.g., delinquency, defaults, accounting losses, etc.).

Reference the location of the comprehensive data dictionary that lists each variable’s description, source, allowable values, and other relevant information.

Response Variable

Describe the response/performance/dependent variable that the model is designed to estimate/project.

Model Owner:

The Alipay fraud detection model is a rule-based system that does not estimate or project a response variable in the traditional statistical or machine learning sense. Instead, it applies predefined rules to assess the risk of fraudulent transactions based on transaction attributes and user behavior patterns.

Explanatory Variables

Describe the explanatory/independent variable candidates assessed in the model development process.

Model Owner:

The Alipay fraud detection model is a rule-based system that evaluates transactions based on predefined criteria rather than statistical estimation of relationships between dependent and independent variables. The model utilizes various transaction attributes and user behavior indicators as explanatory variables to assess fraud risk.

These variables include, but are not limited to, transaction amount, transaction velocity, user authentication details, device information, geographic location, historical transaction patterns, and known fraud indicators. The model applies a set of predefined rules to these attributes to determine the likelihood of fraudulent activity.

As this is a vendor-provided model, the definitions of input variables are aligned with Alipay’s fraud detection framework rather than traditional bank-defined risk metrics like delinquency, default, or accounting losses. While the vendor maintains a detailed data dictionary specifying the description, source, and allowable values for each input variable, these details are not disclosed due to proprietary concerns.

### Data Limitations

Provide information about known data limitations / weaknesses and an assessment of their impact on the final model’s output. For example, if the model was developed based on external data that differs notably from the Bank’s data, the differences and their potential impact must be documented. For each noted weakness / limitation, describe how the associated risk is currently being mitigated. Additionally, where longer-term remedial actions are being undertaken or planned (e.g., an initiative to clean up the existing data or collect incremental data), such actions should also be documented.

Model Owner:

The following data limitations have been identified, along with their potential impact on the model's performance and the steps being taken to mitigate these risks:

* **Differences Between Bank and Vendor Data** – Variations in data structure and granularity between the vendor and the Bank may impact model performance when applied to new data environments. This misalignment can lead to discrepancies in fraud detection. To mitigate this, the vendor conducts a review and acceptance process before implementation and continuously monitors data alignment to address any significant differences.
* **Vendor Data Processing Rules** – The vendor’s proprietary transaction data processing rules have not been fully disclosed, limiting transparency into how inputs influence model outputs. To manage this, the vendor conducts grey testing, allowing for necessary adjustments and ensuring alignment with the Bank’s fraud detection requirements and risk appetite.

### Data Preparation Software / Platform

Provide information on the software and/or programming language used in the data extraction, transformation, and other steps to prepare the model development and testing data. Provide a reference to the location of the development programming codes, associated log files, and other data preparation artifacts.

Model Owner:

The data preparation process for the fraud detection model utilizes the vendor's proprietary platform and software tools for data extraction, transformation, and processing.

Due to the proprietary nature of the vendor’s platform located in China, the exact tools, software, and programming languages used are not disclosed. Additionally, the development programming codes, log files, and other data preparation artifacts are stored and maintained within the vendor's secure environment, and access is restricted for confidentiality reasons.

### Data Retention

Describe where the development data is stored (post development) and how the environment is controlled. Provide the minimum time period for data retention.

Model Owner:

The vendor has not disclosed specific details regarding the retention of data related to the Alipay fraud detection model. As the model is rule-based and does not involve machine learning or AI, data retention requirements may not be explicitly tied to the model itself. However, it is acknowledged that transaction data used for fraud risk assessment may be subject to internal or regulatory data retention policies.

As there is no specific retention protocol shared by the vendor, it is recommended that the Bank ensure compliance with applicable legal, regulatory, and internal requirements related to data retention. The Bank may need to implement its own policies for retaining transaction data and other relevant inputs used in fraud risk assessments for auditing, reporting, and operational purposes.

# CONCEPTUAL SOUNDNESS

## MODEL THEORY AND ASSUMPTIONS

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |
| 3 |  |  |

**Model Assumption Summary**

Please list out model methodology assumptions applied in the model development and model production process, such as missing value treatment, outlier treatment, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Assumption Name** | **Assumption Description** | **Materiality of Assumption** | **Rationales for this Assumption**  (Business driven or quantitative methodology driven) |
| 1 | Missing Value Treatment | Missing values in transaction data are handled by excluding incomplete records from the model input. | Medium | Ensures that incomplete data does not affect model accuracy. |
| 2 | Outlier Treatment | Outliers in transaction amounts (e.g., unusually high or low amounts) are not adjusted or removed, as they are considered valid data points for fraud detection. | High | Fraudulent transactions can exhibit outlier behavior, so they should be preserved. |
| 3 | Data Consistency | Data inputs from transaction payloads are assumed to be consistent and accurate, with no further validation performed on the inputs. | High | Inconsistent data would lead to errors in fraud risk assessment. |
| 4 | Real-time Processing | Assumes that all transaction data is processed in real time, with no delays in the data flow from input to output. | High | Real-time processing is crucial to timely fraud detection and response. |

**Model Limitation Summary**

Please list out model methodology related limitations, their impact of business use, and ongoing monitoring program to appropriately manage the associated risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Limitation Name** | **Limitation Description** | **Impact on Business Use** | **Monitoring Description & Frequency** |
| 1 | Outlier Handling | The model does not adjust or remove outliers in transaction amounts, considering them as valid data points for fraud detection. | It is potential to flag legitimate high-value transactions as fraudulent or miss subtle fraud indicators. | Model performance checks include periodic reviews of transaction data for outliers; along with an assessment of key metrics like detection rate and false positive rate to evaluate the effectiveness. |
| 2 | Historical Data Dependency | The model depends heavily on historical transaction patterns to detect fraud, without considering future fraud trends or real-time risk adjustments. | May fail to identify new, evolving fraud schemes that do not align with past patterns. | Fraud trend analysis through manual review volume and rejection rates, with regular historical data updates for ongoing monitoring. |

### Model Theory and Methodology

#### Modeling Approach

Provide a description of the modeling approach you have selected, including the statistical estimation approach or machine learning technique, if applicable (with further details of the model construction/estimation process to be provided in Section 3.2 Model Estimation/Training and Selection).

For advanced Machine Learning (ML) models, discuss briefly whether a self-explanatory or less complex model (e.g., logistic regression, linear regression) is viable in solving the same business problem. If not, explain why not. Detailed information on this topic should be provided in Section 3.1.1.3. Alternative Approaches Explored

Model Owner:

The Alipay fraud detection model is a rule-based system, meaning that it does not rely on statistical estimation or machine learning techniques. Instead, the model's approach is driven by a set of predefined rules and expert-defined thresholds designed to assess transactions for fraud risk. These rules are based on industry knowledge, regulatory requirements, and historical fraud patterns. As such, this model's construction involves the selection and fine-tuning of these rules rather than statistical modeling or machine learning algorithm training.

Given the nature of the problem—detecting fraud in real-time peer-to-peer (P2P) transactions—a more complex machine learning or statistical model like logistic regression or linear regression would likely not be as effective. These simpler models may not capture the intricate, evolving nature of fraud patterns in the same way a rule-based system can, especially given that fraud detection often requires adaptability to emerging trends and dynamic data. Therefore, while simpler models could theoretically be applied, they would not provide the same level of accuracy and flexibility needed to address the business problem effectively.

#### Model Structure/Formulae

*Detail all relevant mathematical equations applied in the model with a clear explanation of the notation*. Describe the model inputs and outputs if not already provided in Section 2.1.3.5. Variable Definitions

Note: This section applies to all models and should be especially detailed for models that were not developed through statistical or machine learning analysis of empirical data (e.g., the market risk / trading models based on financial theory). For these models, the rationale for the particular choice of inputs (e.g., prices, interest rates, volatilities, variance/covariance matrices) should be provided.

Model Owner:

Faud prevention is focused on identifying and reducing and reducing fraud up front. Detection is a component of prevention, whether the fraud is perpetrated by the actual customer or by a criminal stealing access information and creating a fraudulent remittance.

The Alipay fraud detection model is a rule-based system and does not generate fraud risk scores through mathematical equations or statistical methods. Instead, the system evaluates transactions based on predefined rules and thresholds. These rules are crafted using expert judgment and are designed to identify transactions that exhibit characteristics of potential fraud.

The model inputs typically include transaction details such as senders’ details, transfer details, recipient details and contextual transaction information. These inputs are assessed against the established rules to flag potentially fraudulent activities. The outputs of the model are binary decisions, such as whether a transaction is flagged for manual review or approved for processing.

Since the model does not involve the calculation of risk scores through quantitative techniques, the focus is on the application of expert-defined rules to detect suspicious transactions. The specific thresholds and rule configurations used in the model are proprietary and are based on expert insights into fraud patterns and operational requirements.

#### Alternative Approaches Explored

Describe how the selected model theory/methodology (and estimation technique, if applicable) compares with industry practices for similar models and provide rigorous support for a selected approach that is non-standard or innovative. Provide references to industry and academic publications supporting the choice of this modeling methodology.

Describe alternative modeling approaches (including alternative estimation/numerical techniques, if applicable) that were considered and why they were not selected. Provide references to industry and academic publications discussing the alternative methodologies.

For machine learning (ML) models, provide performance comparison between the self-explanatory model and the selected ML model and a discussion on the trade-offs between model performance and transparency/interpretability. If a self-explanatory model is viable, also provide analysis/test/comparison results with related data/scripts/outputs if any to support the discussion.

Provide a comparative narrative for the selected ML model vs. other comparable/state-of-the-art methodologies with a discussion on the advantages and disadvantages of the selected ML model vs. the alternatives.

Model Owner:

The Alipay fraud detection model is a rule-based system, which operates using a set of predefined rules rather than machine learning techniques. Therefore, there were no alternative modeling approaches such as machine learning (ML) or statistical methods considered and not selected for this particular use case.

The model is easily understood and provides clear, actionable results based on expert knowledge and business intuition. This makes the rule-based system particularly suitable for environments where fraud detection needs to be immediate and where stakeholders require clear reasons for each decision.

Given that the Alipay fraud detection model already meets these operational requirements, no other methodologies were explored or considered as alternatives. The model is built to address the immediate fraud detection needs effectively using predefined rules and thresholds, ensuring it operates efficiently without the complexity and resource requirements associated with machine learning models. Therefore, no performance comparison or trade-off analysis was conducted between machine learning models and the selected rule-based approach.

### Segmentation Approach

Describe and justify the selected model segmentation scheme (or lack thereof), including any related quantitative analyses performed and subject matter expert qualitative considerations. Provide the segmentation waterfall logic, if applicable. Assess the impact of the selected segmentation scheme on the model estimation and output.

If in-model segmentation approach was followed (rather than developing separate equations/model objects for each segment), explain this with the rationale for going the route of in-model segmentation.

Model Owner:

For the Alipay fraud detection model, no specific segmentation approach was employed. The model operates as a rule-based system, and fraud risk detection is carried out using a uniform set of predefined rules applied to all transactions. This is in line with the design of the model, which aims to provide a consistent approach for detecting fraudulent activity across the entire transaction pool.

The decision to not implement a segmentation approach stems from the operational needs of the system, which prioritize simplicity, speed, and interpretability. By using a uniform rule-based system, Alipay ensures that fraud detection is applied consistently across all transactions without the need for complex segmentation logic, which could potentially slow down processing time or introduce inconsistencies in decision-making.

The lack of segmentation also does not negatively impact the accuracy of the fraud detection process, as the rules and thresholds are designed to cover a wide range of fraud scenarios comprehensively. Consequently, no in-model segmentation approach was followed, and all transactions are evaluated uniformly, providing simplicity and operational efficiency.

### Model Settings

If applicable, describe model settings and parameters, including vendor model customizations. For example, a vendor model may offer alternative interest rate term structures for valuation purposes. or a vendor may recommend updated model tuning parameters (e.g., for mortgage prepayment models) to be used in place of default values. For each setting/parameter, justify the selected value relative to the other choices available.

Model Owner:

The Alipay fraud detection model is a rule-based system and does not rely on traditional model settings or parameters commonly found in statistical or machine learning models. Instead, the model’s behavior is determined by predefined rules and expert-defined thresholds designed to detect fraudulent transactions based on historical fraud patterns and real-time transaction data. The vendor has not disclosed specific tuning parameters or adjustments made to these settings due to proprietary concerns.

### Model Assumptions

List and justify the implicit and explicit assumptions associated with the model, including qualitative or quantitative expert judgments. Assess the impact of each assumption to the extent possible. For example, if a model relies on an average of historical values over the last 6 months, it may be important to test the impact on the model output of selecting alternative assumptions, e.g., 3 months, 9 months, etc.

If any assumptions are intended to be conservative, explain in what way they are conservative.

NOTE: Testing of any technical assumptions underlying the selected statistical/machine learning technique should be documented in Section 3.3.1. Statistical and Technical Assumptions Testing.

Model Owner:

The Alipay fraud detection model, being rule-based, operates under several assumptions related to fraud detection patterns and thresholds. These assumptions are shaped by expert judgment and historical data:

* **Fraud Risk Thresholds**: The model assumes predefined thresholds for flagging transactions as potentially fraudulent. These thresholds are based on expert insights into fraud risk and may be adjusted based on emerging patterns. If these thresholds were set too low or too high, the model’s sensitivity to fraud could be compromised.
* **Fraud Behaviour Patterns**: The model assumes that fraud behaviours remain consistent or evolve predictably over time. This assumption relies on expert understanding of fraud trends and the ability to adapt the model to new fraud tactics. If fraud behaviour changes more quickly than anticipated, the model’s accuracy could decrease.
* **Transaction Data Quality**: The model assumes the integrity of input data, such as transaction details, user profiles, and historical behaviour. Any issues with data quality or completeness could reduce the effectiveness of fraud detection.

These assumptions are conservative in that they prioritize minimizing false negatives (undetected fraud) rather than false positives (legitimate transactions flagged as fraud). This conservative approach ensures that fraudulent transactions are flagged even at the risk of a higher number of false alerts, which can be reviewed manually.

### Model Limitations and Weaknesses

List any known model limitations and weaknesses. For each weakness / limitation, there should be a description of the associated model risk and, if applicable, the risk mitigant designed to address this risk. See the following example:

| ***Model Weakness or Limitation*** | ***Associated Model Risk(s)*** | ***Model Risk Mitigants / Remediation*** |
| --- | --- | --- |
| The model output is heavily impacted by several judgmental management assumptions, including x, y, and z. These assumptions are currently lacking empirical support. | Use of judgmental assumptions increases the risk of poor model predictions / measurements and unsupported model estimates, which may lead to inappropriate business decisions. | **Short Term Risk Mitigants**:   1. The judgmental assumptions will be subject to oversight by the governance committee X that will review and challenge the model owner's support for the assumptions on a monthly basis. 2. The model output will be benchmarked to the output from the alternative model Y on a quarterly basis. Significant divergence in the outputs will be investigated.   **Longer Term Remediation Plan**:   1. The model owner will investigate the possibility of obtaining empirical support for the assumptions x and y once an additional 6 months of data are collected. 2. The model owner will investigate the possibility of modifying the modeling approach to reduce the reliance on judgmental assumptions. |

Model Owner:

The Alipay fraud detection model has several limitations:

* **Adaptability to New Fraud Patterns**: The model relies on predefined rules, which may struggle to detect emerging fraud schemes. Regular updates and rule fine-tuning by the fraud detection team are essential to address evolving patterns.
* **Expert Judgment Dependency**: The model depends on expert-designed rules, which can introduce bias, errors, and limited transparency in rule adjustments. To mitigate this, ongoing expert training, periodic audits and detailed documentation of rule changes are necessary.
* **False Positive Rates**: The model's conservative design may result in more legitimate transactions being flagged as fraudulent. A strong manual review process is needed to reduce false positives.

These limitations emphasize the need for continuous monitoring, updates, and oversight to maintain model effectiveness.

|  |  |  |
| --- | --- | --- |
| ***Model Weakness or Limitation*** | ***Associated Model Risk(s)*** | ***Model Risk Mitigants / Remediation*** |
| The model does not adjust or remove outliers in transaction amounts, considering them as valid data points for fraud detection. | It is potential to flag legitimate high-value transactions as fraudulent or miss subtle fraud indicators. | Model performance checks include periodic reviews of transaction data for outliers, performance checks. along with an assessment of key metrics like detection rate and false positive rate to evaluate the effectiveness. |
| The model depends heavily on historical transaction patterns to detect fraud, without considering future fraud trends or real-time risk adjustments. | May fail to identify new, evolving fraud schemes that do not align with past patterns. | Fraud trend analysis through manual review volume and rejection rates, with regular historical data updates for ongoing monitoring. |
| Limited transparency due to rule-based nature | Lack of clear insight into model decision-making process | Documenting rule rationale and establishing validation frameworks |

## MODEL ESTIMATION / TRAINING AND SELECTION

Note: “Model estimation/training” is mostly applicable for those models that rely on statistical estimation and optimization techniques, such as regression analysis or machine learning techniques. However, this section is also relevant to some other types of models, including those that are developed using expert judgment (qualitative models).

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |

### Estimation Methodology and Assumptions

Describe in detail the model estimation methodology, including the assumptions that may be implicit in the estimation technique. For example, ordinary least squares estimations include assumptions about regression residuals. Describe any expert judgments related to the estimation, such as the selection of variable weighting methodologies.

For machine learning (ML) models, discuss whether monotonicity of relationships between the model features and the target variable is important or required, and whether the ML algorithm is configured to ensure such monotonicity.

Model Owner:

The Alipay fraud detection system is based on a rule-based approach, rather than an estimation-based technique like ordinary least squares or machine learning models. The model’s "estimation" process is not based on statistical inference or optimization techniques; rather, it uses predefined fraud detection rules and thresholds designed to identify suspicious or potentially fraudulent transactions. These rules are continuously refined and updated based on feedback and tagged fraud data, ensuring that the system remains effective against evolving fraud patterns.

Since the model is rule-based, there are no explicit assumptions related to statistical methods like regression residuals, multicollinearity, or heteroscedasticity. Instead, the assumptions underlying the system are related to the quality and relevance of the data inputs used in the rules, as well as the effectiveness of those rules in detecting fraud. These rules are crafted by domain experts based on historical fraud data and insights into common fraud schemes, ensuring they remain aligned with evolving trends in fraud tactics.

For machine learning models, which may require the configuration of monotonic relationships between features and target variables, Alipay's fraud detection system does not use machine learning algorithms. Consequently, there are no concerns regarding monotonicity or ensuring the model maintains certain relationships between features and outcomes. The system’s performance relies on consistent rule-based logic, rather than learning from data in the way machine learning models do.

### Modeling Software / Platform

Provide information on the software and/or programming language used in the model estimation/training (including the version number, if applicable). If relevant, list the specific algorithms and packages used in model training.

Model Owner:

The Alipay fraud detection system utilizes a rule-based approach for transaction fraud detection, rather than relying on conventional statistical or machine learning algorithms. As such, the model does not require the use of traditional software platforms for model estimation or training, such as those associated with machine learning or statistical modeling.

The fraud detection system’s rules are embedded within its internal fraud detection platform, which operates on proprietary software designed and maintained by Ant Group. The platform incorporates a variety of fraud detection rules that are continuously refined based on historical fraud data and expert feedback. While specific details regarding the software or platform version are not explicitly shared by the vendor due to intellectual property concerns, the underlying system is built using proprietary technology designed to assess and flag suspicious transactions in real-time.

### Hyper-parameter Tuning

For machine learning models, include a detailed description of the hyper-parameter tuning process, including the following information:

* The approach used for hyper-parameter tuning, including the rationale for leveraging this approach.
* The list of the hyper-parameters tuned (as well as those that are left at default values) and the range of values searched. If applicable, explain why some hyper-parameters were not tuned.
* Performance metric(s) used to select the optimal hyper-parameters and the supporting rationale.
* Sufficiently detailed discussion of the results of the tuning process and selected values, including any judgmental adjustments to the parameters, if any.

If the model also utilizes pre-training during development, provide details of the pre-training process and the pre-trained model as well as related analysis/test/comparison results.

Model Owner:

As a rule-based fraud detection system, the Alipay fraud detection model does not rely on machine learning algorithms or hyper-parameter tuning techniques typically associated with supervised learning models. Instead, the system uses predefined fraud detection rules, which are iteratively refined and updated based on feedback from the internal fraud detection team at Alipay.

Given that the model is not based on machine learning models, there are no hyper-parameters (such as learning rates, regularization parameters, or tree depths) to tune. The "tuning" of the model is focused on updating and refining the fraud detection rules rather than adjusting algorithmic hyper-parameters. These adjustments are made based on historical fraud data, expert judgment, and the evolution of fraud typologies, ensuring that the system remains responsive to emerging fraudulent activities.

Since the model does not utilize pre-training or machine learning model training phases, there is no process for pre-training a model or selecting pre-trained models. Instead, the focus is on enhancing the rules over time through manual refinement and operational testing.

### Feature / Variable Selection

Describe in detail the approaches used to select candidate and final model variables/features, including the relevant criteria/thresholds for quantitative selection criteria, as well as any expert judgments.

Describe the process for involving subject matter specialists from the line of business to obtain their views on candidate variables, including the associated economic theory/business intuition behind each variable, as well as the expectation for the directional impact of each variable on the model output.

Describe any algorithms or statistical procedures (such as correlation analysis, Information Value analysis, stepwise regression procedure, etc.) used as part of the process to select final model variables from the full set of candidate model variables.

Model Owner:

For the Alipay fraud detection model, which is a rule-based system, the approach to feature/variable selection differs from machine learning models that typically rely on algorithmic methods like correlation analysis, stepwise regression, or Information Value. Instead, the model employs a structured approach to variable selection by categorizing key features of event attributes into distinct types which are guided primarily by business requirements, subject matter expertise, and operational performance over time.

According to the vendor, these categories include, but are not limited to:

* **Monetary Features**: Variables that capture financial aspects of transactions, such as amounts and payment values.
* **Transaction Behaviour Features**: Variables that reflect the behavioural patterns of transactions, such as frequency, velocity, and timing.

This categorization helps distinguish between different types of events and allows the model to effectively analyse various aspects of fraud risk. By focusing on these key feature types, the system ensures a comprehensive evaluation of transaction attributes to enhance the accuracy and reliability of fraud detection.

The selection and categorization process are critical for tailoring the model to detect a wide range of fraud typologies, ensuring that the model remains adaptive to different fraud patterns.

### Model Estimation / Training Results

**For statistical models,** provide statistical estimation results for the final model, as well as other model structures that were considered to be strong candidates. Estimation results should include not only the estimated coefficients, but also the t-statistics and associated p-values, measures of model fit, and summary of results of the appropriate statistical diagnostic tests (detailed statistical testing should be documented in the Statistical Testing section).

In addition to providing the estimation results, explain why this model was selected (relative to other candidate models), including both quantitative and qualitative factors.

**For machine learning models:**

* Provide a listing of the full set of features included in the final model.
* Provide a feature importance chart showing the top X most important features in the final model.
* Provide information on the number of features that contribute 90%, 95%, and 99% of model fit. If the number of features providing the last 1-2% of model fit is significant, explain the rationale for their inclusion.

**For both statistical and machine learning models**, this section should contain for each feature an explanation of t he economic theory/business intuition for the inclusion of this feature, as well as the assessment of the estimated directionality of the relationship between the feature and the target variable relative to the a priori expectations. For simple statistical models this assessment can be accomplished through the evaluation of the estimated coefficient signs. For complex statistical and machine learning models, use of explainability testing techniques is required (refer to Section 3.3.5 Model Explainability Testing).

Model Owner:

Since the Alipay fraud detection model is a rule-based system, it does not rely on traditional machine learning techniques like feature importance analysis or model training based on statistical estimation. In this case, the model operates based on predefined rules that assess various factors related to fraud risk.

The feature selection for the rule-based system would have been determined by domain experts or predefined business rules that capture key fraud indicators, such as transaction amount, user behavior patterns, and device or transaction location. These features are typically chosen based on their relevance to the detection of fraudulent activity, but there is no formal process like machine learning-based feature importance analysis involved in this model.

Similarly, the selection of the final model was based on expert judgment and operational requirements. The rule-based system would have been designed to balance accuracy with operational efficiency, with experts determining the specific rules to use based on their knowledge of fraud patterns and business needs. The model's effectiveness would likely have been evaluated through testing, and adjustments to the rules may have been made based on observed performance or changes in fraud patterns.

Thus, the process of selecting the final model and the features used in it is heavily dependent on expert judgment and domain knowledge rather than statistical methods or machine learning algorithms.

#### Judgmental Adjustments

Describe and justify any judgmental overlays/overrides of statistically estimated input parameters. If any such adjustments are intended to be conservative, explain in what way they are conservative. Note: this section should not be used to detail any overlays/overrides to the model outputs (described in Section 3.3.11. Need for Model Overlays).

Model Owner:

The Bank has identified thresholds for individual check transactions attributes, and conditions for generating alerts. Currently there are no judgement overlays and overrides as the model’s materiality is moderate. If judgmental adjustments are required, it will be driven based on the ongoing fraud risk assessment in response to significant risks to the bank.

### Other Types of Model Estimation

#### Model Calibration

If applicable, describe the calibration process for models that are regularly fit to market data.

Model Owner:

For the Alipay fraud detection model, which operates as a rule-based system, the concept of model calibration, as typically applied to statistical or machine learning models, does not directly apply. The model's parameters, including thresholds and rules, are designed based on expert knowledge and predefined criteria rather than being fit or recalibrated based on market data. The system’s behavior and thresholds are periodically reviewed and adjusted by experts to adapt to emerging fraud trends, but these adjustments are not part of a formal calibration process involving market data. Due to the proprietary nature of the model, specific details on any adjustments or reviews are not disclosed.

#### Vendor Model Tuning

If applicable, describe the process and results for any customization of vendor models (e.g., tuning of vendor model behavioral model parameters to Bank portfolio credit or prepayment experience) that is analogous to a statistical estimation.

Model Owner:

For the Alipay fraud detection model, which is a rule-based system, there is no formal process for customization or tuning of model parameters analogous to statistical estimation techniques typically seen in machine learning or other predictive models. The model relies on predefined rules and thresholds designed by the vendor, Ant Group, based on expert knowledge and industry best practices. While adjustments may be made to these rules and thresholds based on emerging fraud patterns or changes in business requirements, these changes are based on expert judgment rather than statistical estimation or calibration to specific portfolio data. As a result, no detailed customization process or results analogous to statistical estimation have been shared, as the vendor considers such information proprietary.

## Model Development Testing

For each test discussed in the following subsections, include the purpose of the test, the testing methodology, the criteria used to evaluate test results (that is, the applicable metrics and thresholds), and a summary of the results with commentary and conclusions. For any anomalous results, the conclusions should include information on the impact of these results on the model outputs and business use, and whether they require any specific risk mitigant.

The level of detail for the testing documentation should be sufficient to provide a clear and definitive basis for the model owner’s conclusions about model’s performance and robustness.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |
| 3 |  |  |

### Statistical and Technical Assumptions Testing

For statistical and any other models that include statistical and other technical assumptions, provide testing of all assumptions associated with the selected estimation technique (e.g., for Ordinary Least Squares models on time series data this includes testing for multicollinearity, heteroscedasticity, non-normality of errors, autocorrelation, non-stationarity, seasonality, etc.).

For vendor models, to the extent that the assumptions testing information is available from the vendor, include the model owner’s assessment of the testing results and any associated risks.

Model Owner:

As the Alipay fraud detection system is a rule-based model, it does not rely on statistical estimation techniques such as Ordinary Least Squares (OLS) or other methods typically used in regression or machine learning models. The model’s operation is based on predefined rules designed to assess transactions for fraud based on a set of attributes, rather than statistical assumptions or estimation procedures.

Given the rule-based nature of the Alipay system, there are no assumptions such as multicollinearity, heteroscedasticity, non-normality of errors, autocorrelation, or non-stationarity that would typically require testing in statistical models. The system’s performance is evaluated through transaction monitoring and feedback loops rather than assumption-based statistical testing.

To assess the model’s effectiveness, the vendor utilizes continuous rule refinement and operational testing. However, no formal statistical assumptions testing is conducted, as the model is not based on these estimation techniques.

Therefore, any associated risks are mitigated through ongoing monitoring, rule adjustments, and the feedback loop used to refine the system's rules over time. The absence of formal statistical assumptions testing is not considered a limitation, given the operational nature of the model and its emphasis on rule-based fraud detection rather than statistical inference.

### Model Performance / Fit Testing

Provide testing of model performance / fit on the estimation and hold-out samples, including calculations of relative and absolute model errors for different population/product/portfolio risk segments and time periods. For some models, their fit can be evaluated using various additional statistical metrics and analytical techniques. This includes, for example: the K-S test, ROC curves (and AUC/Gini coefficient and similar measures of discriminatory power), lift charts, Precision/Recall, F1 score, risk profiling, etc.

For vendor models, include the model owner’s assessment of the model performance/fit testing results provided by vendor (based on vendor’s data) and any associated risks. In addition, include testing results on the Company’s internal data (or explain why it is not feasible).

#### **In-sample Performance/Fit**

Use this section for the testing of model performance/fit on the data on which the model was estimated/trained.

Model Owner:

In-sample performance testing, which would typically involve evaluating the model's fit on the data used for model training, is not directly applicable in the context of the Alipay fraud detection system. The model does not rely on training data in the traditional sense; rather, it applies to a set of predefined rules to assess transactions. However, the rules are continuously refined based on historical fraud data to ensure they remain effective. Although the exact details of in-sample performance testing have not been provided by the vendor, the system's operational performance can be assumed to be assessed through real-time transaction monitoring and feedback loops that help refine rules over time.

#### **Out-of-sample (but not out-of-time)**

Use this section for the testing of model performance/fit on data from the same time period as the in-sample estimation/training data but held out for model testing purposes.

Model Owner:

Out-of-sample performance testing typically involves evaluating the model's ability to generalize to unseen data from the same time period as the training data. For the Alipay fraud detection model, out-of-sample testing is not explicitly detailed, as the system does not use predictive modeling techniques based on past training data. Instead, the model evaluates real-time transactions as they occur, with ongoing refinement based on new fraud patterns. Therefore, specific out-of-sample performance testing, such as K-S tests or AUC measures, does not directly apply to this rule-based system.

#### **Out-of-time**

Use this section for the testing of model performance/fit on data from the time period different from the in-sample data, and not used in the estimation either because it was not yet available at the time of model estimation, or because it was available but excluded from the estimation/training for the express purpose of performing out-of-time model fit testing.

Model Owner:

Out-of-time testing would typically involve testing the model on data from a time period different from the one used in model training, to assess how well the model adapts to new or unseen conditions. Since the Alipay fraud detection model does not rely on training data in the traditional sense, the vendor has not explicitly performed out-of-time testing. However, historical fraud data, which might not be used in rule creation, could still provide valuable insights for the system’s performance in adapting to fraud trends. This is accomplished through ongoing transaction monitoring and rule adjustments, but the absence of formal out-of-time testing means no specific performance metrics or comparative analyses are available.

### Model Stability and Overfitting Testing

Provide testing to assess the stability of the model’s estimated relationships, for example:

* For statistical regression models, this involves regression coefficient stability testing and testing for structural breaks. Coefficient stability testing can be performed by repeatedly re-estimating the model on different subsets of the development sample (e.g., random sub-samples or samples representing different time periods covered by the dataset) as well as out-of-sample / out-of-time datasets. Values of regression coefficients and p-values across all samples are then assessed to evaluate the model stability.
* For machine learning models, because a comparison of model parameters is either impossible or impractical, testing of model stability generally involves a comparison of key performance statistics (e.g., K-S, AUC, Precision, Recall, F1, etc.) on different training and testing datasets. A common technique for assessing machine learning model’s stability and evaluating the risk of model overfitting is k-fold analysis. K-fold analysis should be performed in addition to testing of the model on the training, validation, out-of-sample, and out-of-time datasets.

Model Owner:

As a rule-based fraud detection model, the Alipay system does not rely on statistical regression models or machine learning techniques, so traditional methods of model stability and overfitting testing, such as regression coefficient stability or k-fold cross-validation, are not applicable. Instead, the model's stability is evaluated through continuous operational monitoring and periodic rule refinements.

The Alipay fraud detection model's stability is maintained through the iterative feedback loop that adjusts detection rules based on observed fraud patterns. This process ensures that the system remains adaptive to emerging fraud trends while minimizing the risk of overfitting outdated or irrelevant data.

While there is no formal stability or overfitting testing conducted as typically defined for statistical or machine learning models, the ongoing monitoring of flagged transactions and fraud trends provides an informal assessment of the model's effectiveness. Adjustments are made as necessary to ensure the model continues to meet fraud detection requirements.

### Back-testing

In addition to the model performance/fit testing documented in Section 3.3.2. Model Performance / Fit Testing, back-testing is highly beneficial and should be performed/documented for certain types of models. Back-testing is a class of testing techniques designed to assess the consistency of model predictions/estimations with the actual observed values, especially for different historical periods and over longer testing horizons.

These tests are designed to measure the accuracy of model performance over specified time periods. When documenting back-testing analyses, it is critically important to provide a detailed description of the test design including, for example:

* The design of the testing dataset includes the description of the time period, and information about any notable exclusions/inclusions that are inconsistent with the data used to develop the model.
* The logic for generating model predictions. For example, when back-testing a mortgage default model, the model developer would typically start with a particular historical portfolio snapshot and then use the model to generate predictions for each subsequent month/quarter without truing the model up using subsequent historical data.
* The source and nature of inputs and assumptions used in the back-test. For example, for a model that uses macroeconomic variables as inputs, the typical practice is to use actual historical values of such inputs during the back-test period (in order to isolate the error of the tested model from the error in the economic forecasts).

Use of graphical presentation of actual and predicted values is necessary in addition to any quantitative measures of model error (e.g., MAPE, MSE, etc.). This allows the model developer and reader to observe any areas of persistent model bias.

The developers should ensure that performance metrics and thresholds for acceptable performance are clearly stated and are aligned with the model’s business use. For example, for stress testing or CECL model designed to produce loss forecasts over a 2-year period, one of the error metrics should be based on the cumulative actual vs. predicted losses over a 2-year back-testing horizon.

Back-testing results should be accompanied by detailed narrative providing the model developers’ assessment of said results and their conclusions about any notable model biases or elevated error rates. Some such notable biases and performance issues may need to be noted as model weaknesses that must have associated risk mitigants.

Back-testing should be carried out for different populations. For example, when analyzing performance of residential or commercial mortgage loans, one should separately evaluate performance of the model on sub-populations that can be reasonably expected to have different behavioral characteristics. For example: different products, different vintages, or different segments of population by FICO score or by LTV or by another key risk driver.

Predictive models should also be back-tested over different economic environments, e.g., periods of stress vs. periods of economic growth. This is especially important for stress testing, CECL, and IFRS 9 models.

For vendor models, include the model owner’s assessment of the back- testing results provided by vendor (based on vendor’s data) and any associated risks. In addition, provide testing results on the Company’s internal data (or explain why it is not feasible).

In-time

Use this section for backtesting using the data from the same time period on which the model was estimated/trained.

Model Owner:

As a rule-based fraud detection model, the Alipay system does not undergo traditional back-testing, as it does not generate predictive estimates based on historical data. Instead, the model applies predefined rules to evaluate fraud risk in real time. However, its effectiveness is monitored through transaction outcomes and manual reviews.

The vendor has not provided specific details indicating that in-time testing has been conducted. Since the model operates based on predefined rules, any assessment of its performance would likely be based on ongoing transaction monitoring and case reviews. However, no formal in-time back-testing results or methodologies have been disclosed due to proprietary concerns.

Out-of-time

Use this section for backtesting using data from the time period different from the in-sample data.

Model Owner:

Out-of-time testing, in the conventional sense, is not applicable to this rule-based model, as it does not rely on historical data for predictive modeling. However, historical transaction data and fraud-tagged cases may be periodically analyzed to refine rules and update thresholds. While this iterative process helps improve fraud detection, no structured out-of-time back-testing details have been provided by the vendor.

### Model Explainability Testing

**For machine learning models**, provide sufficient information to understand the drivers of the model outputs and the directionality of their impacts. Use feature importance, Partial Dependency Plots, and a global interpretation method that explains the relationship between model inputs and outputs (e.g., SHAP feature importance, permutation-based feature importance, etc.)

For models that require generation of adverse action reason codes, testing of local interpretability using methods such as LIME is also required.

Advantages and disadvantages of the selected explainability testing methods should be discussed as well.

Model Owner:

As a rule-based fraud detection model, the Alipay system does not rely on machine learning techniques, eliminating the need for traditional explainability testing methods such as SHAP, LIME, or Partial Dependency Plots. Instead, the model's decision-making process is inherently transparent, as it follows predefined rules to assess fraud risk based on transactional attributes.

Each transaction is evaluated against a set of established fraud detection rules, and if a mismatch exceeds the preset risk threshold, the transaction is flagged for manual review. The logic behind these decisions is directly interpretable, as the system applies deterministic criteria rather than learned patterns from data.

Since the model does not generate risk scores or utilize complex statistical relationships between inputs and outputs, there is no requirement for adverse action reason code generation or additional explainability testing. The primary method of validating the model’s effectiveness is through ongoing rule refinement and monitoring of flagged transactions.

### Benchmarking

Compare model results with alternative results using other models and/or other data (if available). Describe the benchmark model or data in sufficient detail to enable an assessment of its value as a reference point. For example, a benchmark model that is also a formal Challenger model that has been independently validated (with a successful validation outcome) would be a stronger reference point than a benchmark model that may be available but that has not been extensively tested. Similarly, external peer data may be more relevant in a benchmark comparison than broader industry data. Provide a detailed narrative explaining the outcome of the comparison and any notable differences between the model outputs and benchmarks.

Model Owner:

As a rule-based fraud detection model, the Alipay system does not undergo formal benchmarking against alternative models, as it operates on predefined fraud detection rules rather than machine learning algorithms. The system’s performance is evaluated through continuous refinement and real-time monitoring, rather than being compared to challenger models or external benchmarks.

There is no formal challenger model with which the Alipay fraud detection system is directly compared. However, the system’s effectiveness is estimated based on transaction outcomes, where flagged transactions are subject to manual review to ensure the accuracy of fraud detection. Feedback from this process informs rule refinement and updates to maintain the model's alignment with emerging fraud patterns.

Given the rule-based nature of the model, comparisons to other models or external data are not performed in the traditional sense. Instead, ongoing feedback loops and operational performance monitoring serve as the primary mechanisms for assessing the model’s effectiveness.

### Sensitivity Analysis

Quantify the impact on model outputs of changes in the value of model inputs and assumptions (e.g., economic inputs, tuning parameters, calculation rules, and scenarios). If the model design is such that the sensitivity of the model output to changes in an individual input would depend significantly on the value of one or more of the other inputs, the impact of simultaneous changes in inputs should also be evaluated.

Model Owner:

As a rule-based fraud detection model, the Alipay system used by East West Bank (EWB) does not involve a formal sensitivity analysis process. The model operates based on predefined rules that are manually set to assess transactions against specified risk thresholds. These rules do not dynamically change in response to variations in model inputs or assumptions.

As the model relies on rule-based decision-making, there is no continuous recalibration of parameters or dynamic input adjustments that would typically require sensitivity analysis. The primary function of the model is to evaluate transaction characteristics (such as amount, geographic location, and sender-recipient patterns) against these established rules. Therefore, changes in input values are directly assessed against the predetermined risk thresholds without the need for sensitivity evaluation across multiple input parameters.

To ensure the ongoing stability and relevance of the system, dashboards and real-time monitoring have been implemented. These tools continuously track flagged transactions and help identify potential risks or operational inefficiencies. However, the model’s design does not require the type of sensitivity analysis typically conducted in more complex, data-driven models where output variance is measured in response to changes in input values.

### Stress Testing / Scenario Analysis

Quantify the impact on model outputs of stressed changes in the values of inputs, including scenarios that are outside the range of ordinary expectations.

For stress testing/CECL/IFRS 9 and other models dependent on economic scenarios, assess the model forecast across benign and stressful scenarios. When evaluating model forecasts under different economic scenarios, the forecasts should be compared to historical values during similar economic conditions (to the extent that such comparison is meaningful). Any notable differences should be explained and justified. For example, if a model produces drastically lower forecasts of losses under a severe stress scenario compared to the historical losses during the Great Recession, an explanation (e.g., notable improvements in the portfolio quality) should be provided and supported with quantitative analysis, where possible.

The forecasts should also be assessed for internal consistency. For example, do the base, adverse, and severely adverse forecasts reflect incremental macroeconomic stress, or, if not, are they consistent with the unique characteristics of the scenarios and business intuition?

For vendor models, stress testing/scenario analysis should be performed on the Company’s internal data. If not feasible, include the model owner’s assessment of the stress testing and scenario analysis provided by vendor (based on vendor’s data) and any associated risks.

Model Owner:

As a rule-based fraud detection model, the Alipay system used by East West Bank (EWB) does not perform traditional stress testing or scenario analysis. The primary function of the model is to identify fraudulent transactions based on transaction characteristics such as amount, geographic location, and sender-recipient patterns. It does not rely on economic inputs, or the types of forecasting used in AI/ML models, which assess the impact of broader economic conditions on forecasts such as credit losses. Therefore, the model does not require stress testing under benign or stressful economic scenarios.

While the model does not undergo formal stress testing, its effectiveness is ensured through continuous performance monitoring. Dashboards track flagged transactions, and real-time monitoring helps identify potential risks or operational inefficiencies. The model’s output is primarily based on the application of rules to transaction data and is adjusted as needed based on evolving fraud patterns.

### Other Testing

Describe other testing performed applicable to the selected modeling approach, **if any**.

Model Owner:

As a rule-based fraud detection model, the Alipay system undergoes ongoing rule refinement and operational testing. These activities ensure that the predefined fraud detection rules remain effective and adapt to emerging fraud trends. Apart from this, no additional performance testing details have been explicitly shared by the vendor, as the approach described focuses primarily on rule refinement and operational testing to maintain the system’s fraud detection capabilities.

### Overall Performance Assessment

Discuss overall conclusions on model performance based on the results of the testing described above.

Model Owner:

As a rule-based fraud detection model, the Alipay system undergoes ongoing rule refinement and operational testing. These activities ensure that the predefined fraud detection rules remain effective and adapt to emerging fraud trends.

As the model is rule-based, testing primarily involves evaluating the efficiency and accuracy of the rules in detecting fraudulent transactions. Periodic reviews of transaction patterns and feedback from manual reviews help identify areas where rules may need to be updated or refined. This testing process is not conducted on historical data in the traditional sense but relies on continuous, real-time feedback to ensure the model's effectiveness.

Additionally, operational tests are performed to assess the system’s ability to handle large transaction volumes and flag suspicious activities without significant delays. These tests ensure that the system performs efficiently under normal and peak transaction loads.

The exact details of these tests have not been explicitly shared by the vendor due to intellectual property concerns.

### Need for Model Overlays

Document any proposed or implemented adjustments or overlays to the model outputs and their rationale. Describe the process for derivation and application of these overlays. Provide the impact by including model results with and without these overlays. Finally, outline the overlay review & challenge/approval process, including any Senior Management / Committee reviews and approval process if applicable, and the frequency of the overlay re-evaluation.

For vendor models, discuss the need for model tuning/dialing settings to better align model outputs to the Company’s internal outcomes.

Model Owner:

The Bank has identified thresholds for individual check transactions attributes, and conditions for generating alerts. Currently there are no judgement overlays and overrides as the model’s materiality is moderate. If judgmental adjustments are required, it will be driven based on the ongoing fraud risk assessment in response to significant risks to the bank.

# PRODUCTION PROCESS COMPLETENESS & ACCURACY

This section includes procedures and information related to model testing and usage following model development or vendor model acquisition.

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |
| 3 | digital-banking-bc-plan\_02\_07\_2025\_11\_39-pdf | Business continuity plan |

## Production Application Testing

Describe the testing for accuracy of implementation of the model into production systems.

### System Testing Approach and Results

The objective of model production application testing is to ensure that computational processes implementing model calculations:

* Are consistent with the documented model specifications produced as part of the model development process. This includes source data fields, data transformation rules, mathematical equations, assumption values, etc.
* Are consistent with the documented business / user requirements.
* Are mathematically accurate and complete.
* Have been reviewed for consistency with any applicable accounting/finance specifications (e.g., GAAP and/or accounting policy requirements), stress testing requirements, or any other applicable regulatory requirements.
* Are operationally stable, repeatable, and sustainable.
* Interface accurately with both upstream and downstream systems (where applicable).

For vendor models, the purpose of the production application testing is to ensure that the models are correctly implemented on the Bank’s systems—if on-premises production process is selected, or the vendor’s model production environment is correctly connected to the Bank’s production data environment—if a cloud-based production process is selected, that the Bank’s production data inputs are consistent with the model publisher’s input specifications, and that all applicable software patches and fixes have been applied.

Describe in detail the testing plan for the individual model’s production implementation and its integration within a larger system and the vendor’s model production environment, if applicable. Include User Accepting Testing cases and scenarios, expected outcomes, and the individuals responsible for executing the test cases.

Document the results of the UAT testing execution, and the associated log of issues and subsequent resolutions.

Model Owner:

For the Alipay fraud detection model, the testing plan focuses on ensuring that the model is correctly implemented within the vendor's cloud-based environment. Given that the model is rule-based and does not rely on data used for training, the testing approach involves validating that the system’s historical transaction patterns, adjusted for the Bank’s risk appetite, are correctly applied.

The testing process includes the following key steps:

* **Rule Review and Acceptance**: Before implementing the fraud detection rules, a comprehensive review and acceptance process is conducted, ensuring that the rules align with the Bank’s objectives and risk appetite.
* **Gray Testing**: The vendor performs gray testing, which involves gradually introducing the new rules in batches, allowing for monitoring and assessment of the model’s performance in a controlled environment.
* **Monitoring and Adjustments**: The system is monitored to ensure that the rules function as intended, and any necessary adjustments are made to optimize performance.

### User Acceptance Testing Approach and Results

Document the User Acceptance Testing approach, results, and sign-offs.

Model Owner:

The User Acceptance Testing (UAT) for the Alipay fraud detection model follows a structured approach to ensure its proper implementation and functionality within the Bank’s systems. Initially, acceptance criteria are defined based on the model’s objectives and business requirements. Test cases are created using historical data or user samples and executed in a controlled environment to check the system’s ability to detect fraud.

A Proof of Concept (POC) phase validates the system’s functionality, gathering feedback from users on usability. Any issues identified are tracked and resolved. A formal sign-off is required before the system moves to production.

Following the UAT phase, a post-UAT review is conducted to capture lessons learned and to improve future testing processes. This review ensures that the testing approach continues to evolve and refine for future model implementations.

## Model Production Specifications

The following technical specifications should cover the end-to-end operation of the model, from data inputs and assumptions to final model reports. **To avoid duplication of information, some of the following sections may refer to earlier document sections instead of repeating the information.**

### Model Platform

Describe the technologies used for running the model, for example, Python, R, Excel, etc.

Model Owner:

The Alipay fraud detection model operates on the vendor's in-house technology and platform, which is specifically designed for real-time fraud detection. Due to proprietary concerns, the vendor is unable to disclose detailed information regarding the specific technologies or platforms used.

### Data and Process Flow Diagram

Provide a flow diagram showing data sources, inputs, quality assurance control points, intermediate results, outputs, and reports.

Model Owner:

The vendor (Alipay) has not explicitly provided a process flow diagram. However, based on the information available about Alipay's rule-based fraud detection system, a basic outline of the logical process flow is presented below:

**Transaction Data Input:** The data for each remittance transaction (including transaction details, customer profiles, and other relevant factors) is input into the fraud detection system via the Digital Banking platform (mobile apps or online banking).

**Data Processing:** Transactions are evaluated against the predefined fraud detection rules.

**Analysis:** Transactions are flagged based on whether they meet the risk criteria defined by the model’s rules.

**Manual Review:** Transactions flagged for high risk are sent for manual review by Alipay’s operational fraud detection team.

**Decision Output:** After review, the decision is made whether to approve or reject the transaction based on the fraud risk score and manual review insights.

### Input Data Specifications

Provide a list of all inputs, including measurement units, a description of valid values or ranges (a full data dictionary should be attached in an appendix). Describe any data processing rules, such as filtering missing or invalid values infilling / overrides, substituting ceiling or floor values, data transformations, etc.

Model Owner:

Below is a sample of the transaction payload shared by EWB to Alipay for processing. The input data is structured as follows:

**1. Sender Details:**

* **AccountType**: Type of the sender's account (e.g., checking, savings).
* **ReferenceId**: Unique transaction reference ID.
* **CustomerNumber**: Identification number of the sender.
* **AccountNumber**: Sender's account number.
* **AccountCurrentBalance**: Current balance in the sender's account.
* **RoutingNumber**: Routing number for bank transactions.
* **Address**: Sender's address.
* **FirstName**: Sender’s first name.
* **LastName**: Sender’s last name.
* **AccountId**: Unique ID for the sender's account.
* **AccountRelCode**: Relationship code for the account.

**2. Transfer Details:**

* **Amount**: The amount being transferred.
* **Currency**: The currency type used in to initiate Alipay Transfer (e.g., USD).
* **StartDate**: Date when the transfer starts.
* **ExpectedDeliveryDate**: Expected date for the transfer to be completed.
* **ExchangeID**: The exchange ID for foreign transactions.
* **ReceiverAmount**: Amount to be received by the recipient.
* **ToReferenceId**: Unique reference ID for the recipient’s transaction.
* **WireDeliveryMethod**: The method used for wire transfer (e.g., SWIFT, ACH).
* **IsVerifyOnly**: Flag indicating if the transfer is verification-only or an actual transaction.
* **Purpose**: Purpose of the transaction (e.g., personal, business).
* **Type**: Type of the transfer (e.g., domestic, international).
* **RecevierCurrency**: Foreign Exchange Currency Code (e.g., CNY)
* **FxRate**: The foreign exchange rate, if applicable.
* **Mode**: Mode of transaction (e.g., online, in-person).
* **TransferSpeed**: Speed of transfer (e.g., standard, expedited).
* **SubPurpose**: Subcategory for transaction purpose.
* **Notes**: Any additional notes or remarks related to the transfer.

**3. Recipient Details:**

* **TelephoneNo**: Recipient's telephone number.
* **Email**: Recipient’s email address.
* **IsNewRecipient**: Flag indicating if the recipient is new.
* **CustomerNumber**: Unique identifier for the recipient.
* **AccountNumber**: Recipient's account number.
* **SwiftCode**: SWIFT/BIC code of the recipient’s bank.
* **ExternalID**: External identifier for the recipient.
* **AccountRelCode**: Relationship code for the recipient’s account.
* **BankAddress**: Address of the recipient’s bank.
* **FirstName**: Recipient's first name.
* **IsMyAccount**: Flag indicating if the recipient is the same as the sender.
* **Address**: Recipient's address.
* **ReceiverCurrency**: Currency in which the recipient will receive the funds.
* **AccountType**: Account type of the recipient.
* **Type**: Type of the recipient’s account.
* **BankDetails**: Additional details of the recipient’s bank.
* **IntermediaryBankDetails**: Details of intermediary bank if applicable.
* **PhoneCountryCode**: Country code of recipient’s phone number.
* **LastName**: Recipient’s last name.
* **RecipientID**: Unique ID for the recipient.

**Data Processing Rules:**

The specific data processing rules related to the handling and validation of transaction payloads, including any filtering, in-filling, or substitution practices, are proprietary to the vendor and cannot be disclosed.

This payload, provided by EWB to Alipay, serves as a sample of the data used in the fraud detection process.



### Model Formulas / Algorithms

Describe detailed model formulas, algorithms, and numerical techniques, if possible.

Model Owner:

The Alipay fraud detection system is a rule-based model that does not rely on traditional numerical algorithms or formulas. The model utilizes predefined business rules rather than standard machine learning or statistical algorithms for fraud risk assessment.

While the vendor has not disclosed the specific internal logics due to proprietary concerns, the core mechanism involves applying transaction rules based on transaction details such as sender, recipient, amount, currency, exchange rate, and other attributes. These rules are designed to identify potentially fraudulent activities by assessing transaction patterns, historical transaction behavior, and other predefined risk factors.

The model’s output is based on these risk rules, which continuously adapt based on operational feedback, rather than being driven by complex mathematical formulas or algorithmic calculations.

### Model Parameters and Settings Values

Provide the values for all parameters and other input assumptions, including hyper-parameters for machine learning models.

For vendor models, specify values of user-selectable settings.

Model Owner:

For the Alipay fraud detection system is a rule-based model, there are no traditional machine learning hyperparameters or machine learning model settings like in an AI-based model. The model operates on predefined, static rules that are based on historical transaction data patterns and aligned with acceptable risk appetite. These rules assess the likelihood of fraud based on factors such as transaction amounts, recipient details, transfer speeds, and other parameters, but specific values for thresholds are proprietary and not disclosed by the vendor.

There is no machine learning models or user-selectable settings in this rule-based system, and as a result, no hyper-parameters or model parameters are available for external review. The system is continuously adjusted to adapt to changing fraud patterns and operational needs, but the exact configurations remain confidential.

### Model Outputs

Provide a list of all model outputs, including expected values or ranges.

Model Owner:

The output of the Alipay fraud detection system is based on whether a transaction meets the predefined rules in the model. If the transaction passes all the fraud detection rules, it is approved for processing. However, if the transaction does not comply with the rules, it is flagged as suspicious and moved to manual review by the fraud detection team. The decision-making process is binary: the transaction is either approved or flagged for manual review, depending on whether it adheres to the model's fraud detection criteria. This ensures that suspicious transactions are further investigated before being processed.

### Reports

Provide a list of all standard output files or reports and describe how they are used in the business.

Model Owner:

The Alipay fraud detection system generates reports that include transaction approval or flagging status. If a transaction matches the defined fraud rules, it is approved; if not, it is flagged as suspicious and moved to manual review. These reports help the fraud detection team prioritize and investigate flagged transactions. The system ensures that flagged transactions are closely monitored to detect potential fraud. The reports are crucial for tracking transaction outcomes and supporting manual fraud investigation.

## Operational Controls

Operational controls related to the model should be in place prior to the production deployment of the model.

### Model Access and Security

Access controls prevent unauthorized changes to the production code and unauthorized operation of the model in production. Describe who has “write access” to the model and can make changes to the underlying code of the model in development and in production, who has access to run the model in production, and who controls model access rights. If there is a formal access monitoring and review process in place, describe it here. Indicate whether any model files are password protected.

If there is no technical mechanism to prevent changes to the model in production (e.g., if the model is implemented using Python code), describe any checks performed to verify that no unauthorized changes have been made since the last approved update or use of the model (such as code comparisons).

Model Owner:

Alipay's fraud detection system utilizes robust access controls to ensure that unauthorized changes to the production code are prevented. Only authorized personnel have “write access” to the model during both the development and production stages. The access rights to modify the model or make updates are managed by a designated access control team within Alipay. The fraud detection team, who is responsible for operating the model in production, does not have access to alter its underlying code.

Model access rights are controlled by the internal team at Alipay, and any changes are subject to strict internal procedures. The company has formal access monitoring and review process in place to ensure that no unauthorized changes occur. Any potential modifications to the model are carefully monitored and reviewed.

Although the specific details of the system protection are not disclosed, security protocols ensure that unauthorized access is prevented. If any technical mechanisms, such as manual checks, are in place to verify model integrity, these are closely managed to ensure that the model runs as intended without unauthorized alterations.

### Production Deployment

Describe the production deployment process for the new model or changed model, including related controls.

Model Owner:

The production deployment process for the Alipay fraud detection system follows a structured and controlled approach. Before any model changes are deployed to production, thorough testing is conducted to ensure the model functions as intended within the production environment. This includes reviewing and validating the new or updated rules against historical data or sample transactions, followed by a period of gray testing to observe performance under real-world conditions.

Once testing is complete and all necessary approvals are obtained, the updated model or rule set is deployed incrementally, often affecting a limited portion of online traffic initially. This gradual rollout helps ensure that any unforeseen issues are detected early and can be mitigated before full deployment. The deployment process includes detailed monitoring to track the system's performance and detect any anomalies or unexpected behavior.

Furthermore, access to the production environment is tightly controlled, with changes only made by authorized personnel. Any changes or updates to the model are documented, and production deployment is only finalized after all steps have been completed successfully and reviewed for compliance with internal standards.

### Model Usage Controls

Describe the controls related to model usage, such as verification of inputs (including reconciliation to the general ledger or other reference data, as applicable), confirmation of successful model execution (e.g., all input records were processed, output values are within valid ranges), completion of hand-offs to downstream users of the model’s outputs, etc.

Model Owner:

The model usage controls for the Alipay fraud detection system include several key measures to ensure the accuracy and integrity of the model's inputs, execution, and outputs. First, inputs to the model, such as transaction data, are verified for completeness and accuracy before being processed. This includes validation checks to confirm that the necessary transaction details, like sender and recipient information, are provided and within expected formats.

Once the model executes, verification procedures ensure that all input records have been processed and that the output values, such as transaction approval or flagging, fall within valid and expected ranges. Any discrepancies or failures in execution trigger alerts for review by authorized personnel, ensuring that the system remains reliable and consistent.

For hand-offs to downstream users, such as the fraud detection team, clear and documented procedures are in place. This ensures that flagged transactions are properly transferred for manual review and that any necessary follow-up actions are taken promptly. Additionally, there is an established process for reporting on model performance and outputs, which helps stakeholders stay informed and take corrective actions when required.

### Model Backup

Provide the model backup procedures, including parties involved and frequency, and describe how the model owner has determined that the procedures are functioning correctly.

Model Owner:

The vendor has not explicitly provided details regarding the model backup procedures. As part of the overall deployment process, the model undergoes a review and acceptance process before being deployed. However, specific information on backup procedures, such as frequency, location, and recovery processes in case of system failure, has not been shared.

Given the vendor's control over the model execution environment, it is assumed that backup procedures are part of the standard operational practices, but no detailed information on the specifics of backup and disaster recovery planning was disclosed.

## Contingency Plans

### Disaster Recovery Plan

Provide a reference to the disaster recovery plan or describe the plan here.

Model Owner:

The East West Bank (EWB) Digital Banking Disaster Recovery Plan (DRP) defines procedures for restoring IT systems, data, and infrastructure following a disruption. The DRP focuses on minimizing downtime and ensuring that critical banking services are restored promptly.

The DRP includes specific Recovery Time Objectives (RTOs) for different systems, with Tier 1 systems requiring recovery within 4 hours, Tier 2 within 1 day, Tier 3 within 3 days, and Tier 4 exceeding 3 days.

Key aspects of the DRP include:

* Application Recovery: The IT team assesses system disruptions, identifies affected applications, and coordinates recovery efforts. Tier 1 systems, including customer-facing websites and fraud detection tools, are prioritized for rapid restoration.
* Data Backup and Restoration: Digital banking applications rely on AWS, Azure, and on-premises data centers. Backups are maintained, and recovery plans include procedures for data restoration and loss mitigation.
* Failover Mechanisms: Critical applications have automatic failover to backup systems or alternative cloud environments. AWS and Azure services can be redeployed in different locations if needed.
* Incident Response & Communication: The Network Operations Center (NOC) monitors IT systems 24/7, troubleshoots issues, and coordinates with subject matter experts. Disruptions are escalated based on severity, and affected departments are notified through the Business Continuity Incident Hotline.
* Third-Party Dependencies: The DRP addresses recovery strategies for third-party services such as LexisNexis, FIS, and Alipay, which support fraud detection and payment processing. If a third-party service is disrupted, EWB escalates issues with vendors and applies manual workarounds when applicable.

This DRP framework ensures that East West Bank’s digital banking services, including fraud detection models like Alipay, remain resilient and operational in the face of disruptions. For detailed information, please refer to the attached document.



### Business Continuity Plan

Provide a reference to the business continuity plan or describe the plan here. For a vendor model, provide the plan for how the model will be supported or replaced if the external vendor is no longer available to support the model or the vendor’s level of service is unsatisfactory.

Model Owner:

The EWB Digital Banking Business Continuity Plan (BCP) provides a structured approach to maintaining essential business functions before, during, and after a disruption. BCP is designed to protect critical banking operations, minimize risk exposure, and ensure compliance with regulatory requirements.

The plan outlines specific strategies for:

* Incident Response & Reporting: Employees must report business continuity incidents through the BCP Hotline. The Crisis Management Team (CMT) is activated for significant disruptions. Life safety measures take priority in emergencies.
* Workforce Recovery: If critical personnel become unavailable, staffing priorities are reassessed. HR is notified to initiate the replacement process in case of extended workforce disruptions. This may involve internal role-reassignments or external hiring. HR receives details on role descriptions, required experience, and system access needs.
* Technology & Location Dependencies: Digital banking services depend on AWS, Azure, and on-premises data centers. If a location becomes inaccessible, employees work remotely or relocate to an alternate EWB facility.
* Third-Party Dependencies: The BCP acknowledges reliance on external vendors, including Alipay, LexisNexis, and Salesforce, for fraud detection, identity verification, and customer service. If a vendor service is disrupted, EWB applies alternative solutions or escalates the issue.
* Return to Business as Usual (BAU): Once recovery objectives are met, the Department Recovery Team conducts an after-action review to document lessons learned and improve the BCP for future incidents.

This BCP framework ensures that East West Bank’s digital banking services, including fraud detection models like Alipay, remain resilient and operational in the face of disruptions. For detailed information, please refer to the attached document.



## Operating Procedures / User’s Guide

Provide step-by-step procedures for running the model, which may include:

1. Input data extraction and preparation, including data cleaning and transformations.
2. Checking the correctness of input data.
3. Setting/updating/checking model settings, assumptions, and parameter values.
4. Checking the correctness of the settings, assumptions, and parameter values.
5. Initiating the processing component of the model.
6. Checking successful completion of the model execution.
7. Extracting model outputs.
8. Checking that model outputs are valid.
9. Producing standard reports.
10. Distributing standard reports.

Note: if there is a separate operating procedural document (or User’s Guide), please list the document name below and share the document with MRM.

Model Owner:

The Alipay fraud detection system operates as a rule-based, real-time model. The model's execution follows a structured process to ensure accuracy and reliability.

1. **Input Data Handling**: Transaction data is received and verified for completeness, ensuring that required fields such as sender and recipient details, transaction amount, and account information are provided.
2. **Validation Checks**: The system performs automated checks to confirm the correctness of input data, ensuring all values conform to expected formats.
3. **Model Execution**: The model applies predefined fraud detection rules to the transaction data in real time.
4. **Processing and Decisioning**: If the transaction meet the approval criteria, it proceeds. If any fraud indicators are triggered, the transaction is flagged as suspicious and routed for manual review by the fraud detection team.
5. **Output Validation**: The system verifies that all transactions have been processed and that flagged transactions are appropriately identified.
6. **Reporting and Distribution**: The results are logged, and flagged transactions are made available to the fraud detection team for further analysis. Any standard reports generated are distributed to relevant stakeholders.

The vendor has not shared a separate operating procedures document due to proprietary concerns.

# ONGOING MODEL GOVERNANCE & OUTCOME ANALYSIS

**Reference Document List**

Please list all the documents referred to in this section.

|  |  |  |
| --- | --- | --- |
| **#** | **Reference Document Name** | **High Level Description and purpose of the Document** |
| 1 | f02 MRM-CONTROL01 - y&n Model Assmt Fraud 059- Charles Lin YesM- Alipay | Enterprise risk management and Model risk classification procedures. |
| 2 | MRM-CONTROL02 - Model-IRR Assmt 059 -M- Charles Lin - Alipay 2024 | Model inherent risk rating assessment form. |

## Ongoing Risk & Performance Monitoring Plan

**Part 1** - provide an overview of the performance monitoring process, including:

1. Frequency of monitoring activities.
2. Titles/positions of individuals/teams responsible for executing performance monitoring analyses.
3. Individuals responsible for evaluating the resulting reports and documenting conclusions.
4. Stakeholders responsible for reviewing the performance reports and initiating required actions in the event that new risks or performance weaknesses are detected.

**Part 2** - provide the details of the **ongoing risk and performance monitoring plan (together, ongoing monitoring plan)** for this model. Ongoing monitoring plans should generally cover the following two types of periodic monitoring activities:

1. Model Risk Monitoring – Reassessment of the model’s risk profile. This includes but is not limited to reassessment of model weaknesses and limitations, as well as the associated risk mitigants in light of any changes in the model use, Company’s strategy, market conditions, and regulatory environment, among other things.
2. Model Performance Monitoring – Analysis of the model’s **predictive performance** and **identification of emerging model performance weakness**.

Specifically, for Model Performance Monitoring design, it is expected that all models should have some type of outcomes-based performance monitoring process in place to evaluate whether the model is meetings its designed objectives. The Model Owners must specify, as appropriate and feasible for the specific model and its individual uses, detailed plans to monitor model performance through **some combination of the following** four methods:

* Comparison of predicted outcomes to actual values (i.e., back-testing).
* Benchmarking model outputs against comparable external data points, such as observable market information, or outputs of alternative models.
* Analysis of sensitivity of model outputs to variations in model inputs, parameters, and assumptions.
* Stress testing of model predictions to extreme changes in model inputs and assumptions.

The Model Owner should define performance thresholds which, if breached, would require the Model Owner to take corresponding actions. Performance thresholds may be set based on business unit policies or procedures, judgmentally, or based on statistical methodology utilizing model performance over the development sample. In all cases, the approach for setting performance thresholds should be established during development and documented in this section.

**Guidelines** for Risk & Performance Monitoring Plan details:

* Risk Monitoring Plan Details: The risk monitoring plan should list the internal and external factors that should be considered when evaluating model risks. This may include, as applicable:
  + - * Changes in the model use.
      * Changes in the portfolio composition or characteristics of the portfolio/asset/liability/transactions to which the model is being applied.
      * Changes in the Company's strategy.
      * Industry and economic environment changes.
      * Regulatory environment changes.
      * New regulatory findings, independent model validation findings, internal audit findings, external audit findings etc. The plan should include a list of internal and external stakeholders, groups, and committees that may identify, either directly or indirectly, model-related risks through their own “ordinary course of business” activities. It is expected that the Model Owner will establish and maintain periodic communications with these stakeholders to monitor emerging risks.
    - Performance Monitoring Plan Details: The performance monitoring plan should include:
* The source(s) of data used in the performance monitoring process.
* The list of key performance metrics that will be calculated and reported along with their technical specifications.
* Description of the performance analysis that will be performed consistent with the requirements.
* Acceptable performance thresholds for each key metric, if applicable. If a specific threshold is not defined, the Model Owners should document the justification for the lack of threshold. The Model Owners’ rationale for selecting particular performance thresholds must be adequately documented. If, as is sometimes the case, an oversight committee is required by the Business Unit/Line of Business to approve model performance thresholds, then this fact must be reflected in the monitoring plan and the Model Owners must retain evidence of such approvals. Finally, the frequency of the re-evaluation of the performance thresholds should be documented.
* Procedures for communicating and escalating performance issues to appropriate stakeholders (committees, upper management, etc.).
* Procedures for responding to performance threshold breaches.
* The list of stakeholders (individuals and committees) responsible for the review of the risk and performance reports.

Part 1 – Overview

|  |  |
| --- | --- |
| Frequency of monitoring activities (e.g., monthly, quarterly, etc.) | Quarterly Cadence |
| Titles/positions of individuals/teams responsible for executing performance monitoring analyses | Fraud risk management team and operational fraud analysts. |
| Individuals responsible for evaluating the resulting reports and documenting conclusions | Internal fraud analysts and operational risk teams. |
| Stakeholders responsible for reviewing the performance reports and initiating required actions in the event that new risks or performance weaknesses are detected | Business risk teams, compliance teams, and fraud operations management. |

Part 2 – Risk & Performance Monitoring Plan

Model Risk Monitoring Plan Details:

Model Owner:

Model risk monitoring aims to proactively identify and mitigate risks in the scoring system used for decision making, while model validation verifies that models perform as expected in line with design objectives and business uses. The comprehensive approach includes monitoring rules performance, tracking errors, assessing rule modifications, performance tracking, regular reviews, and stakeholder reporting. Through both Ongoing Performance Monitoring (OPM) and validation processes, the bank ensures models remain sound, identifies potential limitations and assumptions, assesses their possible impact, maintains data integrity, and addresses risks promptly to sustain a reliable and effective decision-making system.

* However, fraud detection rules are periodically reassessed to ensure they align with evolving fraud trends, regulatory expectations, and business requirements.
* The effectiveness of the rule-based system is reviewed in response to changes in transaction patterns, emerging fraud tactics, and compliance mandates.
* Any updates to the rule set undergo validation before deployment to minimize unintended impacts.

Model Performance Monitoring Plan Details:

Model Owner:

**Cadence with the vendor**

Cadence with the vendor is regular interactions and activities that will help manage and maintain the ongoing performance monitoring. This includes:

**Regular Meetings:** Quarterly check-ins, to discuss performance and address issues.

**Performance Reviews:** Quarterly evaluations or reviews, to assess the vendor’s performance against agreed-upon metrics and standards.

**Focus:** Quarterly model performance to keep both parties informed about progress and potential concerns. Establishing a clear cadence with your vendor helps ensure transparency, accountability, and continuous improvement in the partnership. It allows both parties to stay aligned, address issues promptly.

**Monitoring Frequency:** Quarterly cadence with the vendor, discuss model performance and evaluate metrics such as false positive rates, detection rates, and manual review volume.

Since this is a **rule-based model**, performance adjustments rely on expert-driven modifications rather than algorithmic retraining. If performance weaknesses are identified, rule modifications are made to improve fraud detection accuracy while minimizing disruptions to legitimate transactions.

## Model Approval and Change Management Process

In this section, discuss the aspects of the model approval and change management process that are specific to this model.

### Model Approval Process

Provide the names of the individuals (or a committee) involved in the approval process for this model.

Model Owner:

Alipay is a managed solution, meaning Ant Group controls mobile and online payment and is responsible for the global fraud detection model and not custom for the bank.

Ongoing cadence to ensure Alipay notifies and provides impact assessment, discuss key updates and governance controls.

### Model Change Log

Provide a reference to the model Change Log. Please refer to the Bank’s 1st Line Model Risk Management Guidelines (MRM-PnP05), the MRM Procedure (MRM-PnP02), and Model Change Log Template v01.docx for detailed requirements.

Model Owner:

Adopted the MRM model change-log template to capture the nature model changes, reasons for the model changes, and potential model impacts. Using this model change-log template to ensure modifications are managed in a framework, minimizing risks, maintaining model integrity to align with MRM quarterly model change certification process. Added risk impact column in the log to provide transparency in the potential impacts.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change Date** | **High-Level Description of Change** | **Change Impact** | **Category of Change** | **Responsible Party** | **Supporting Documents & Location** | **Communication and Approval** | **Additional Comments** |
| NA | NA | NA | NA | NA | NA | NA | NA |

The proposed changes are prompted by changes in fraud patterns, inherent risks, regulatory requirements, business strategies or technical advancements. Each category of change will have different levels of model risk impact.

# APPENDICES

## Appendix A

List and describe references to additional model-related files that have not already been referenced in the Template.

1. DocName\_1.pdf (doc, txt, xls, etc.)

Description: xxx

1. …

Model Owner: NA

## Appendix B

For vendor models, provide high level description of the vendor company background, qualifications, and services provided, especially relating to EWB’s purchase. In addition, please reference MRM procedure MRM-PnP04, MRM-PnP04 EWBC MRM Vendor Model Onboarding Process v01.pdf, for detailed onboarding and documentation requirements.

Model Owner:

The vendor providing the Alipay fraud detection system is **Ant Group**, a global leader in digital payment and financial technology solutions. Ant Group specializes in risk management, fraud prevention, and secure transaction processing for digital financial services.

The Alipay fraud detection system is a **rule-based model** designed to evaluate transactions against predefined fraud detection rules. If a transaction meets the approval criteria, it is processed successfully; otherwise, it is flagged as suspicious and sent for manual review by the fraud detection team. The system operates in real time, ensuring that potentially fraudulent transactions are identified and reviewed before completion.

Ant Group provides **robust fraud management capabilities** that integrate seamlessly with financial institutions’ existing infrastructure. While the system does not generate fraud risk scores, it effectively identifies suspicious transactions by leveraging continuously updated fraud rules tailored to evolving fraud patterns.

For **EWB's purchase**, Ant Group’s services include the implementation of the **Alipay fraud detection system**, which enhances EWB’s ability to manage fraud risks by enabling real-time transaction screening and manual review when needed. The system is designed to support secure and efficient fraud detection processes, helping EWB mitigate fraud risks in its digital banking operations.