Fraud Risk Management Policy

1. Introduction

The Fraud Risk Management Policy ("Policy") of KLM Axiva Finvest Limited is established to outline the processes, procedures, and mechanisms required to identify, assess, prevent, detect, report, and manage fraud risks across the Company. This policy adheres to the provisions of the Reserve Bank of India Master Directions on Fraud Risk Management in Non-Banking Financial Companies (NBFCs) (including Housing Finance Companies) dated July 15, 2024.

The Policy is intended to establish a comprehensive approach to fraud risk management, maintaining the highest standards of integrity and transparency in operations of the company, ensuring that measures are in place to prevent and manage fraud risk effectively.

2. Objectives

The primary objectives of this Fraud Risk Management Policy are to:

- Establish a strong internal control framework to prevent, detect, and mitigate fraud risks.
- Maintain a high level of vigilance across the company to identify potential fraud activities.
- Protect the company's assets, reputation, and stakeholders by minimizing exposure to fraud.
- Foster a culture of transparency, accountability, and integrity within the organization.
- Ensure compliance with legal requirements, including adherence to principles of natural justice during fraud investigations.

3. Roles and Responsibilities

Board of Directors: The Board is responsible for approving the Fraud Risk Management Policy, ensuring its implementation, overseeing the risk management framework's effectiveness and guaranteeing that fraud risk management practices align with regulatory requirements.

Committee of Executives (CoE): Committee of Executives shall oversee the effectiveness of the fraud risk management and review and monitor cases of frauds, including root cause analysis, and suggest mitigating measures for strengthening the internal controls, risk management framework and minimising the incidence of frauds. Committee of Executives (CoE) consist of below members:

1. Whole-time Director
2. Chief Executive Officer
3. General Manager
4. Chief Information Officer
5. Chief Vigilance Officer
6. Head – Internal Audit
7. Head – Operations

Internal Audit Department: The Internal Audit Department will periodically assess the effectiveness of internal controls, audit business processes, and identify fraud vulnerabilities.

Employees: All employees are required to comply with the fraud risk management procedures, report any suspicious activities, and act with integrity in all professional dealings.

4. Fraud Prevention Measures

The Company adopts the following measures to prevent fraud:

Risk Assessment: Conduct periodic fraud risk assessments to identify vulnerable areas in the organization where fraud may occur.

Employee Training: Trainings and awareness programs for employees on identifying fraud and ethical behaviour.

Internal Controls: Implement a robust system of internal controls, including segregation of duties, authorization protocols, and regular reviews of financial transactions.

Technology Solutions: Utilize advanced fraud detection systems, such as data analytics and AI-based fraud detection, to monitor transactions in real-time.

Anti-fraud Culture: Promote an ethical organizational culture where fraud is strictly prohibited, and employees feel empowered to report any suspicious activity.

5. Early Detection of Frauds

The Company implements the following mechanisms for early detection of fraud:

Fraud Risk Monitoring: Continuous monitoring of transactions and financial activities to detect anomalies indicative of fraud.

Early Warning Signals (EWS): Establish and implement an Early Warning Signals framework to identify potential fraud risks at an early stage. This may include indicators like sudden changes in business patterns, mismatches in financial data, or unusual transactions. The EWS will be aligned with the risk profile of each business segment. Risk Management Committee shall oversee the effectiveness of the framework for EWS. The Senior Management shall be responsible for implementation of a robust Framework for EWS.

Audits and Inspections: Regular audits and inspections of operations, especially in high-risk areas, to detect fraudulent activities.

6. Early Warning Signals (EWS) Framework

Early Warning Signals (EWS) are proactive indicators that help in identifying potential fraud risks or vulnerabilities before they escalate into actual fraudulent activities. The Company will establish a systematic process for capturing, evaluating, and responding to EWS.

6.1 EWS Identification

The Company will use a combination of transactional, behavioural, and environmental indicators to define EWS, which may include but are not limited to:

- Transaction-Level Indicators**:**
  - Unusually large or rapid transactions that deviate from the client's typical transaction patterns.
  - Multiple failed attempts or inconsistencies in login credentials.
  - Sudden increase in the frequency or volume of transactions.
  - Transactions with entities or accounts flagged for suspicious activity.

- Behavioural Indicators**:**
  - Employees displaying signs of unusual behaviour, such as financial distress, secretive conduct, or unusual absenteeism.
  - Employees showing a pattern of non-compliance with internal controls or approval processes.

- Customer-Related Indicators**:**
  - Incomplete or inconsistent documentation during the onboarding process.
  - High-risk customers engaged in activities or transactions outside of their declared business scope.
  - Frequent changes in account details, such as address or contact information or other KYC details.

- Operational Indicators:
  - System glitches or failures that consistently affect high-risk transactions or functions.
  - Unexpected changes in key personnel in positions responsible for handling sensitive transactions.

6.2 EWS Monitoring Process

To ensure continuous monitoring of potential fraud risks, the Company will:

Leverage Technology: Use fraud detection systems, data analytics, to monitor real-time transactions and flag unusual patterns or activities as potential EWS.

Cross-Functional Collaboration: Coordinate with various departments (such as operations, internal audit, and IT) to monitor and identify emerging risks and red flags.

Periodic Risk Assessments: Conduct Periodic risk assessments, which will incorporate the evaluation of EWS indicators and their relevance to the Company's operations.

Review EWS Reports: The CoE will review EWS reports and prioritize them for investigation and corrective actions, ensuring swift response to potential fraud risks.

6.3 Response to EWS

Once an EWS is identified, the Company will follow a structured process for addressing the signal:

Initial Review: The identified EWS will be reviewed by the relevant functional team. A decision will be made on whether the EWS requires further investigation decided by the CoE.

Investigation: If the EWS is deemed significant, an internal investigation will be initiated. The investigation will follow due process, ensuring that the principles of natural justice are upheld, and all involved parties are given a fair opportunity to present their case.

Mitigation Measures: If a fraud risk is confirmed, corrective measures will be implemented to address the vulnerability. This may include strengthening internal controls, enhancing employee training, or modifying operational processes.

Escalation: If necessary, the matter will be escalated to the Risk Management Committee or the Board and, where applicable, reported to external authorities and regulators.

7. Procedural Safeguards and Compliance with Natural Justice Principles

In line with the Master Directions, the Company shall ensure compliance with the principles of natural justice while dealing with fraud allegations. The following measures will be adopted:

7.1 Issuance of Show Cause Notice (SCN)

When fraud is suspected, the Company shall issue a detailed Show Cause Notice (SCN) to the alleged persons, entities, and their promoters/whole-time/executive directors under examination.

The SCN shall provide complete details of the transactions, actions, or events that lead to the contemplation of fraud, including any documentary evidence that forms the basis of the allegation.

7.2 Reasonable Time for Response

A reasonable time of not less than 21 days shall be given to the recipients of the SCN to respond to the notice.

The response should be submitted in writing, addressing the allegations, and may include supporting documents or justifications.

7.3 System for Issuance of SCN and Examination of Responses

The Company shall have a structured process for the issuance of SCN and for reviewing the responses. This will include internal discussions, an assessment of the facts, and proper documentation of all decisions made in the process.

The CoE shall oversee the examination and investigation of fraud allegations, ensuring compliance with regulatory requirements.

7.4 Reasoned Order/ Classification

After the receipt and review of the response to the SCN, a reasoned order shall be issued by the Company on whether the account or entity is classified as fraudulent or not. The reasoned order shall include:

- Details of the transactions/actions/events leading to the fraud allegation.
- Responses or submissions made by the concerned persons/entities.
- Reasons for classifying the entity or account as fraud or otherwise, supported by relevant facts and circumstances.

8. Reporting of Frauds

All instances of fraud shall be reported to the relevant regulatory authorities in accordance with the regulatory guidelines.

8.1 Reporting of Frauds to Law Enforcement Agencies (LEAs)

The Company shall immediately report the incidents of fraud to appropriate LEAs, viz. State Police authorities, etc., subject to applicable laws.

8.2 Reporting of Incidents of Fraud to Reserve Bank of India (RBI)

The Company shall furnish Fraud Monitoring Returns (FMRs) in individual fraud cases, irrespective of the amount involved, immediately but not later than 14 days from the date of classification of an incident / account as fraud.

The 'date of classification' is the date when due approval from the competent authority has

been obtained for such a classification, and the reasoned order is passed.

Updates to the FMR shall be provided through FMR Update Application (FUA). The Company shall close fraud cases using 'Closure Module' where the fraud cases pending with LEAs/Court are disposed of and the examination of staff accountability has been completed.

8.3 Reporting Cases of Theft, Burglary, Dacoity and Robbery

The Company shall report instances of theft, burglary, dacoity and robbery (including attempted cases), to Fraud Monitoring Group (FMG), Department of Supervision, Central Office, Reserve Bank of India, immediately (not later than seven days) from their occurrence.

The Company shall also submit a quarterly Return (RBR) on theft, burglary, dacoity and robbery to RBI using online portal, covering all such cases during the quarter. This shall be submitted within 15 days from the end of the quarter to which it relates.

8.4 Reporting of Incidents of Fraud to other Regulators/Authorities

Applicable instances of frauds shall be reported to Stock Exchanges, SEBI or other Applicable Authorities.

9. Corrective Actions

The company shall take the following corrective actions in the event of fraud:

Recovery of Losses: Take steps to recover financial losses resulting from fraudulent activities.

Disciplinary Actions: Employees found guilty of fraud shall face appropriate disciplinary actions, which may include termination of employment, legal action, and financial penalties.

Systemic Changes: If necessary, modify business processes, controls, and procedures to mitigate the risk of recurrence of similar fraud incidents.

10. Whistle blower Protection

The Company has a dedicated Vigil Mechanism/whistle blower Policy that allows employees and third parties to report suspicions of fraud confidentially ('protected disclosures'). All whistle blower reports will be investigated in strict adherence to the principles of confidentiality, integrity, and fairness.

11. Legal Audit of Title Documents

The Company shall implement a periodic legal audit and re-verification of title deeds and other related documents for credit facilities of Rs. 1 crore and above, throughout the tenure of the loan until it is fully repaid.

The scope and frequency of legal audits will be determined by the Board, in line with best practices and legal requirements. These audits will assess the validity of title deeds, security interests, and ensure compliance with applicable laws. The findings from the legal audit will be reviewed by senior management, and corrective actions will be taken if any issues are identified.

12. Provisioning /Write off

1. The following personnel
    a) Head – Internal Audit
    b) Head – Operations
    c) Chief Vigilance Officer
    d) Head – Legal
    e) Branch Manager/Regional Manager/Zonal manager

shall present reports to the Committee of Executives of the account or entity classified as fraud including details of amount involved, amount recovered/recoverable, insurance, possible loss to the Company, etc.

2. The Committee of Executives shall present a consolidated report on the fraud identified to the Executive Director or Chief Executive Officer.
3. Executive Director or Chief Executive Officer shall place the consolidated report on the fraud to the Board of Directors.
4. The Board of Directors shall instruct the Chief Financial Officer on the amount of provision to be made or written off in the financial statements.
5. The CoE shall also present a quarterly update (from the date of detection to the end of the quarter) of the account or entity classified as fraud to the Executive Director or Chief Executive Officer.

13. Periodic Review of Fraud Risk Management Policy

The Board of Directors shall review this Policy at least once every three years, or more frequently, as necessary.

Approved by the Board of Directors on October 30, 2023;
Revised by the Board of Directors on March 18, 2025.