

Corporate Office: Plot No. A9, Sector 3, Noida - 201301
Registered Office: CP-3, Sector-8, IMT Manesar,
Gurgaon, Haryana-122051
Tel: +91 120 3667180
CIN: U65923HR2008PTC046947
www.hcl.com

VAMA SUNDARI INVESTMENTS (DELHI) PRIVATE LIMITED

Fraud Risk Management Policy

**(Approved by the board of directors at its meeting held on
September 30, 2020 & reviewed on 16th March, 2021, 15th
March, 2022, 20th March, 2023 ,9th December, 2024, 18th
December 2025 and 31st March 2026)**

Version Control	
Policy Approval Authority	Board of Directors
Document Author	Risk Department
Document Reviewed by	RMC
Version	7.0
Document Date	December 2025
Review Frequency	Annual

Contents

1. Introduction	3
2. Objective	3
3. Scope	3
4. Definitions	4
5. Governance and Roles & Responsibilities	4
6. Prevention and Early Detection	5
7. Early Warning Signals (EWS) Framework	6
8. Indication of fraudulent activities- Credit facility/ Loan account/ Other financial transaction	8
9. Independent Confirmation from the third-party service providers including professionals	8
10. Staff Accountability	9
11. Issuance of show cause notice and passing reasoned order	9
12. Reporting of Frauds to Law Enforcement Agencies (LEAs)	9
13. Reporting of Incidents of Fraud to Reserve Bank of India (RBI)	9
16. Confidentiality	12
17. Review and Updates	12
18. Retention of records	12
Annexure 1: - SOP for issuance of show cause notice and passing reasoned order after taking the decision on Fraud/No Fraud Declaration	12

1. Introduction

Vama Sundari Investments (Delhi) Private Limited (VAMA) has a commitment to high legal, ethical and moral standards. All members of staff are expected to share this commitment. This policy is established to facilitate the development of procedures which will aid in the investigation of fraud and related offences.

Fraud Risk Management policy is outlined in accordance with the RBI guideline on Fraud Risk Management vide RBI/DOS/202425/120DOS.CO.FMG.SEC. No.7/23.04.001/2024-25 dated 15.07.2024 along with any amendments, clarifications, notifications, or instructions issued by RBI or any other applicable laws from time to time. VAMA provides loans only to its subsidiaries and group entities, therefore the fraud risks primarily relate to internal financial reporting, related party transactions, documentation integrity, misuse of authority, and diversion or misapplication of funds by group entities

2. Objective

- Establish a structured approach to prevent, detect, and respond to fraud risks.
- Foster a culture of honesty, accountability, and strong ethical values within the organization.
- Comply with the RBI's Master Directions on FRM applicable to NBFCs and any other relevant regulations.
- Ensure timely and effective fraud reporting to the Board, regulators, and other stakeholders as required.
- Protect the company's assets and reputation.
- Maintain zero tolerance for internal fraud and ensure that all lending to subsidiaries is supported by valid documentation, Board approved terms, compliant related party governance and accurate financial disclosures.

3. Scope

This policy applies to all directors, employees, consultants, contractors, vendors, and any other stakeholders associated with the company, especially governing the activities of company.

Fraud risk management covers all types of fraud—financial, misconduct, misreporting, collusion, and cyber fraud—that can arise in relation to the company's functions. The scope covers all intercompany loan transactions, interest calculations, documentation flows, approvals, reconciliation of balances, monitoring of end use of funds lent to various borrower entities and compliance with related party frameworks under

Companies Act and RBI directions. This policy applies to all outsourced accounting, audit or financial service providers engaged by the company.

4. Definitions

- **Fraud:** As defined under the RBI Master Directions and Companies Act, 2013, fraud includes any intentional act or omission, including any misrepresentation or concealment of facts, used to deceive, cause wrongful gain or loss to the company or other persons.
- **Fraud Risk:** The possibility of occurrence of fraud that may cause loss to the company.
- **Fraud Incident:** Any instance or suspected instance of fraud detected or reported.
- **Date of Occurrence:** Date when the actual misappropriation of funds has started taking place, or the event occurred, as evidenced / reported in the audit or other findings.
- **Date of Detection:** Actual date when the fraud came to light in the concerned branch / audit / department, as the case may be, and not the date of approval by the competent authority of the company.
- **Date of Classification:** Date when due approval from the competent authority has been obtained for such a classification, and the reasoned order is passed.
- Misapplication of group funds, diversion of loan proceeds, unauthorised withdrawals, fabrication of supporting documents and manipulation of intercompany accounting shall be considered fraud incidents.

5. Governance and Roles & Responsibilities

5.1 Board of Directors

- Approve and sponsor the FRM policy and framework.
- Review and monitor fraud risk management effectiveness.
- Ensure adequate resources for fraud risk management.
- Oversee reporting of fraud cases.

Corporate Office: Plot No. A9, Sector 3, Noida - 201301

Registered Office: CP-3, Sector-8, IMT Manesar,

Gurgaon, Haryana-122051

Tel: +91 120 3667180

CIN: U65923HR2008PTC046947

www.hcl.com

5.2 Audit Committee

- Annual review of fraud risk management mechanisms.
- Assess reports on incidents of fraud and corrective actions.
- Recommend improvements to Board.

5.3 Senior Management

- Implement and maintain the FRM framework.
- Ensure adherence to policies and regulatory requirements.
- Conduct fraud risk assessments.
- Promote a culture of ethical behaviour and zero tolerance to fraud.
- Ensure all group lending transactions are executed strictly as per Board approval and ensure controls to prevent unauthorised changes in loan terms, interest rates or repayment schedules,

5.4 Fraud Risk Management Committee (FRMC)

- Constituted as Special Committee of the Board for Monitoring and Follow-up of cases of Frauds' (SCBMF) consist of three member and one being the whole time director of the company.
- Oversee the effectiveness of the fraud risk management in the company
- Review fraud incidents, investigate and recommend corrective action.
- Ensure proper maintenance of fraud risk registers and controls.

5.5 Employees

- Adhere to the FRM policy and internal controls.
- Immediately report any suspicion/knowledge of fraud.
- Participate in fraud awareness programs.

6. Prevention and Early Detection

The company has in place, systems and procedures in place which are applied diligently for prevention and early detection of frauds. The following are some sources detecting fraud:

- Review of MIS preparation, dissemination

- Reconciliation of accounts
- Monitoring of investments
- Periodic internal audits
- Statutory audit
- Other Early warning signals
- Defined approval workflow to initiate and execute transactions and ensure no staff has unilateral authority to approve or amend any related party loan terms.

In addition to the above-mentioned sources for detection of fraud, cases reported through following may also be taken into consideration:

- **Whistleblower policy:** Employee should be encouraged to report fraudulent activity in the company along with the reasons in support of their views under the Whistle Blower Policy.
- **Role of Auditors:** The auditor may immediately bring instances where the transactions in the account or the documents point to the possibility of fraudulent transactions in the account, to the notice of the top management and if necessary to the Audit Committee of the Board (ACB) for appropriate action.

7. Early Warning Signals (EWS) Framework

7.1. Objective

The Company shall maintain an Early Warning Signals (“EWS”) Framework as part of its Fraud Risk Management framework to facilitate early identification, monitoring and reporting of potential fraud risk indicators in credit transactions.

7.2. EWS Framework – Credit Facilities / Loan Accounts

The Company shall monitor loan accounts and credit exposures for identification of early warning indicators which may indicate financial stress, irregular conduct, diversion of funds or potential fraud.

The following indicators shall, inter alia, be monitored:

- a. Repayment Behaviour of the Borrower - non-repayment or delay in servicing of loans beyond agreed timelines, requests for restructuring of loan/credit facility;

- b. Financial position of the borrower – parameters such as profitability, net worth, debt service coverage, liquidity etc. shall be monitored;
- c. Unusual or unexplained utilisation or diversion of funds;
- d. Material legal, regulatory or compliance issues concerning the borrower;
- e. Conduct issues - Delay or non-submission of financial information, confirmations or other data sought by the Company, change in auditors etc.;
- f. External/Market intelligence – any adverse news related to the borrower or negative industry outlook.

Generation of any EWS trigger shall require examination by the Risk function to assess whether the account requires further review from fraud risk perspective. Significant observations shall be escalated to the Fraud Risk Management Committee and to the Board.

7.3. EWS Framework – Other Financial / Non-Credit Related Transactions

- a. **Investment decisions** – transactions outside Board-approved investment policy, mandate, or exposure limits; frequent unexplained deviations from stated investment strategy or asset allocation;
- b. **Fund transfers and settlement** – delays or failures in pay-in/pay-out, and mismatches between contract notes, bank statements, and demat/custodian records;
- c. **Banking transactions** – payments or transfers to accounts/beneficiaries not forming part of the Company's approved/registered payee list; unauthorised or unexplained changes to registered bank account/mandate details; transactions inconsistent with the Company's usual banking pattern (unusual value, frequency, or timing); unauthorised access to or usage of net-banking/payment credentials;
- d. **Reconciliation** – unresolved or recurring discrepancies between the Company's internal records and bank/custodian/depository statements.

7.4. Monitoring and Governance

The EWS Framework shall be reviewed at least annually, or as required to ensure its continued relevance and effectiveness.

The Company shall maintain appropriate records of EWS alerts, reviews conducted, observations noted and actions taken thereon.

8. Indication of fraudulent activities- Credit facility/ Loan account/ Other financial transaction

The company will monitor financial and other financial transactions and remain alert on activities, which could potentially turn out to be fraudulent

- In case where there is a suspicion / indication of wrongdoing or fraudulent activity, company shall use an external audit (Auditors who are qualified to conduct audit under relevant statutes.) / internal audit as per board approved policy for further investigation in such cases or accounts.
- In case where audit report submitted remains inconclusive or is delayed due to non-cooperation by the party (person/entity accused of fraud), company shall conclude on status of the party as a fraud or otherwise based on the material available on their record and their own internal investigation / assessment in such cases (after adhering to principles of natural justice).
- In case a party (person/entity accused of fraud) is identified as a fraud by the company, other group companies, in which one or more promoter(s) / whole-time director(s) are common, shall also be subjected to examination by company from fraud angle.
- In cases where Law Enforcement Agencies (LEAs) have suo-moto initiated investigation involving a party (person/entity accused of fraud), company shall follow the process of classification of account as fraud in accordance with the board approved fraud risk management policy.

9. Independent Confirmation from the third-party service providers including professionals

Company may rely on various third-party service providers as part of its routine business activity. Therefore, Company shall be incorporating necessary terms and conditions in their agreements with third-party service providers to hold them accountable in situations where willful negligence / malpractice by them is found to be a causative factor for fraud. Agreements with professional service providers will include clauses on accuracy of certification, liability in case of misstatement and support during fraud investigations.

10. Staff Accountability

It is essential to identify the erring official/s immediately on detection of a fraud and conclude the disciplinary action/ departmental action expeditiously; especially in frauds where staff involvement is seen and punishment commensurate to the crime/ lapses should be awarded to such fraudsters.

In that context 'Staff Accountability' shall be examined in line with company HR policy.

Once staff accountability is examined disciplinary action shall be initiated and concluded as per HR policy of the company

11. Issuance of show cause notice and passing reasoned order

In case company has classified an incident as fraud, the company shall serve detailed show cause notice to the persons, Entities and its Promoters / whole-time and Executive Directors against whom allegation of fraud is being examined with complete details of transactions, / actions / events basis which declaration and reporting of a fraud is being contemplated in accordance with SOP for issue of show cause notice(refer annexure 1).

12. Reporting of Frauds to Law Enforcement Agencies (LEAs)

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

In terms of establishing a single point of contact, Head of Legal shall be the nodal officer for reporting of incidents of frauds and interaction with law enforcement agencies with the help of other stake- holders.

13. Reporting of Incidents of Fraud to Reserve Bank of India (RBI)

- i. **The company will select the most appropriate category of fraud from the below mentioned list to ensure uniformity and consistency while reporting incidents of fraud to RBI through Fraud Monitoring Returns (FMRs) using online portal:**
 - a. Misappropriation of funds and criminal breach of trust;
 - b. Fraudulent encashment through forged instruments;
 - c. Manipulation of books of accounts or through fictitious accounts, and conversion of property;
 - d. Cheating by concealment of facts with the intention to deceive any person and cheating by impersonation;

- e. Forgery with the intention to commit fraud by making any false documents/electronic records;
- f. Wilful falsification, destruction, alteration, mutilation of any book, electronic record, paper, writing, valuable security or account with intent to defraud;
- g. Fraudulent credit facilities extended for illegal gratification;
- h. Cash shortages on account of frauds;
- i. Fraudulent transactions involving foreign exchange;
- j. Fraudulent electronic banking / digital payment related transactions committed on NBFCs; and
- k. Other type of fraudulent activity not covered under any of the above

Modalities of reporting incidents of fraud to RBI

- l. Company will furnish FMR 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.
- m. Company shall adhere to the timeframe prescribed in the Master Directions for reporting of fraud cases to RBI. Company shall examine and determine staff accountability for delays in identification of fraud cases and in reporting to RBI.
- n. While reporting frauds, company shall ensure that persons / entities who / which are not involved / associated with the fraud are not reported in the FMR.
- o. Company may, under exceptional circumstances, withdraw FMR / remove name(s) of perpetrator(s) from FMR. Such withdrawal / removal shall, however, be made with due justification and with the approval of Board.
- p. Frauds perpetrated in group entities shall also be reported to RBI separately, if such entities are not regulated or supervised by any financial sector regulatory/ supervisory authority. The group entities will have to comply with the principles of natural justice before declaration of fraud.

ii. Closure of fraud cases reported to RBI in FMR

- a. Company shall close fraud cases using 'Closure Module' where the actions as stated below are complete
 - The fraud cases pending with LEAs / Court are disposed of; and
 - The examination of staff accountability has been completed.

- b. Company shall, for limited statistical / reporting purposes, to close those reported fraud cases involving amount upto ₹25 lakh, where examination of staff accountability and disciplinary action, if any, has been taken and:
- The investigation is going on or charge-sheet has not been filed in the Court by LEA for more than three years from the date of registration of First Information Report (FIR); or
 - The charge-sheet is filed by the LEAs in trial court and the trial in the court has not commenced or is pending before the court for more than three years from the date of registration of FIR.
- c. In all closure cases of reported frauds, company shall maintain details of such cases for examination by auditors.

Compliance department shall be responsible for ensuring the reporting and closure of cases in the Fraud Monitoring Report (FMR) submitted to the Reserve Bank of India (RBI). Additionally, compliance team headed by the CCO shall provide regular status updates to the Fraud Risk Management Committee(Special Committee) regarding identified fraud incidents, reporting progress, investigation status, and case closure.

14. Reporting Cases of Theft, Burglary, Dacoity and Robbery

1. To 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.
2. Submission of quarterly Return 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.

15. Other Instructions

i. Role of Auditors

During the course of the audit, auditors may come across instances where the transactions in the account or the documents point to the possibility of fraudulent transactions. In such a situation, the auditor should immediately bring it to the notice of the senior management and if necessary, to the Audit Committee of the Board (ACB) of the company for appropriate action. Further, audit committee shall review the findings of any internal investigations by the internal auditors into matters where there is suspected fraud or irregularity or a failure of internal control systems of a material nature and reporting the matter to the board.

Internal Audit of the company shall cover controls and processes involved in prevention, detection, classification, monitoring, reporting, closure and withdrawal of fraud cases, and weaknesses observed in the critical processes in the fraud risk management framework of the company.

Also, the role of auditors shall be in conformity of Rule 13 of The Companies (Audit and Auditors) Rules, 2014.

16. Confidentiality

All information pertaining to any suspected or confirmed fraud incident shall be handled confidentially and shared strictly on a need-to-know basis. All documents shared by subsidiaries during investigations will be secured and access restricted.

17. Review and Updates

This Policy shall be reviewed at least annually or when there are significant regulatory or operational changes such as material change in the lending structure or related parties, etc. Updates or amendments will be approved by the Board of Directors.

18. Retention of records

All fraud incidents along with the results of investigation relating thereto shall be retained by the Company for a minimum period of 7 years from the date of closure of cases.

Annexure 1: - SOP for issuance of show cause notice and passing reasoned order after taking the decision on Fraud/No Fraud Declaration

Standard Operating Procedures (SOP) shall adhere to the principle of natural justice and the following procedure shall be followed.

1. Competent Authorities defined for different levels of investigation of Fraud.
 - a. Initiating Authority- This shall be Competent Authority for (i) serving Show Cause Notice on the directions of Final Authority, (ii) scrutinizing party's representation on Show Cause Notice for onward submission of its views &

opinion to Reviewing Authority and (iii) communicating the decision of 'Fraud/ no fraud' to the party after final decision of Final Authority.

- b. Reviewing Authority- Competent Authority for perceiving 'Fraud/ No Fraud' in the account based on recommendations of Initiating Authority (IA).
 - c. Final Authority (FA)- Competent Authority authorizing issuance of SCN, taking decision of 'Fraud/ No Fraud' based on the facts presented and passing comprehensive reasoned order in the account.
2. Competent Authorities for serving Show Cause Notice, perceiving fraud, taking final decisions in accounts and passing reasoned order are as under:

Fraud Amount	Initiating Authority	Reviewing Authority	Final Authority
Up to INR 3 Cr	CCO-1	CCO	CRO
Above INR 3 Cr	CCO	CRO	FRMC (Special Committee)

3. Process of serving show cause notice and reasoned order is as follows:
- a. Based on the findings of investigation reports (Preliminary/ Detailed Investigation/ Forensic Audit/ routine investigation, complaint enquiry, suo-moto, through RBI/DFS or other references), a note shall be placed before Final Authority covering the facts of the case, only if fraud is perceived with the party.
 - b. If Final Authority suspects fraudulent connotations, it shall authorize to issue Show Cause Notice indicating the grounds for suspecting fraud, which will be communicated by Initiating Authority. The Initiating Authority will issue Show Cause Notice to the party within 7 days of authorization by Final Authority.
 - c. A timeline of 21 days will be provided to the party to respond to Show Cause Notice from the date of receipt of the notice and if reply is not received within aforesaid stipulated timeline or notice remains unserved or party refuses to accept it, the company shall proceed unilaterally and the proceedings initiated by the company will be treated as ex-parte.
 - d. Where the Final Authority decides 'No Fraud' in the account, no Show Cause Notice shall be issued.
 - e. Show Cause Notice to be served as per the table above.
 - f. The Show Cause Notice/ Reasoned order will be sent by the Initiating Authority on the directions of Final Authority through in person/Speed Post/ Registered Post with acknowledgement due.

Corporate Office: Plot No. A9, Sector 3, Noida - 201301

Registered Office: CP-3, Sector-8, IMT Manesar,

Gurgaon, Haryana-122051

Tel: +91 120 3667180

CIN: U65923HR2008PTC046947

www.hcl.com

- g. Relevant proof (i.e., receipt of Speed post/Regd. AD) of serving of Show Cause Notice/ Reasoned order through all the modes shall be held on record. It is advisable that instead of waiting for receipt of Acknowledgements/ undelivered notices/ service report from the Post Office, company (investigating official) to track service of these notices from the website of Indian Post of the Govt. of India <https://www.indiapost.gov.in> and download the report for maintaining record.
 - h. The Show Cause Notice/ Reasoned order will be sent to the registered address of the party as per companies' records. No separate SCN needs to be issued to third party/guarantor, if their involvement is not ascertained in perpetration of fraud. However, a copy of SCN issued to party to be furnished to the guarantor for information.
 - i. Relevant extract of the Forensic Audit/ Preliminary/ Detailed Investigation/ any other as decided by Initiating Authority, may be shared along with the Show Cause Notice except sensitive internal information viz. role of staff members, role of third-party entities, internal policies/ procedures of the company, etc.
-