SBI CAPITAL MARKETS LIMITED

FRAUD RISK MANAGEMENT POLICY

Registered Office: SBI Capital Markets Limited, 1501, 15th floor, A & B Wing, Parinee Crescenzo Building, G Block, Bandra Kurla Complex, Bandra East, Mumbai- 400 051 | Tel: 4196 8300 |
Email: corporate.office@sbicaps.com
Web: www.sbicaps.com | CIN: U99999MH1986PL040298

SBI CAPITAL MARKETS LIMITED

Fraud Risk Management Policy

1. Preamble:

In the Group Risk Management meeting held in January 2015, SBI has suggested that a suitable policy for SBI Capital Markets Limited (hereinafter referred to as "**SBICAP**" or "**the Company**") be drawn up and approved by the Board on Fraud Risk Management. The Policy was introduced on 31st July 2015.

2. Statement of Purpose and Objective:

In view of the above and to prevent, detect and monitor the fraud risk in the Company, the Fraud Risk Management Policy is framed. The Policy lays down effective mechanisms to prevent, detect and monitor the fraud risks in the company.

The main objectives of the Policy are:

a. Establishing a fraud risk governance model
b. Establishing the roles and responsibilities of the fraud risk management mechanism
c. Instituting a pro-active fraud risk management culture and a preventive fraud risk framework
d. Comply with all relevant legislation and regulatory requirements relating to fraud risk and reporting
e. Create fraud risk awareness and training philosophy

3. Scope:

This policy applies to all the Employees (including those on deputation and contract) as well as external vendors and contractors of SBICAP.

4. Definition of fraud:

According to Oxford Dictionary Fraud means "Wrongful or criminal deception intended to result in financial or personal gain.'
The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery, and extortion.

Further, as per Section 447 of Companies Act 2013, 'fraud' includes:
any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any ***wrongful gain*** *or* ***wrongful loss****.*
*"**Wrongful gain**" means the gain by unlawful means of property to which the person gaining is not legally entitled.*
*"**Wrongful loss**" means the loss by unlawful means of property to which the person losing is legally entitled.*

5. Abbreviations:

Term	Description
C&RM	Compliance and Risk Management
CAG	Comptroller and Auditor General
DCM	Debt Capital Market
DOP	Document of Procedures
ECM	Equity Capital Market
HR	Human Resources
IT	Information Technology
KYC	Know Your Customer
MD&CEO	Managing Director and Chief Executive Officer
P&COO	President and Chief Operating Officer
PASF	Project Advisory & Structured Finance
RBI	Reserve Bank of India
SBI	State Bank of India
SBICAPS	SBI Capital Markets Limited
SEBI	Securities and Exchange Board of India
SVP	Senior Vice President
CRO/GCRO	Chief Risk Officer / Group Chief Risk Officer

6. Nature and types of fraud:

There are many types of corporate frauds, including the following common frauds:

- Theft / misappropriation of cash, funds, or physical assets
- Misuse of accounts
- Procurement fraud
- Payroll fraud
- Payoffs and kickbacks
- Financial accounting misstatements
- Inappropriate journal vouchers
- Suspense accounting fraud
- Fraudulent expense claims
- False employment credentials
- Bribery and corruption
- Data leakage/ theft/ and other information security related malpractices
- Forging Documents / Signatures
- Falsifying documents
- Fraudulent dealing through forged instruments, manipulation of books of account or through fictitious accounts and conversion of assets.
- Unauthorised Trading/Investment activities with intent to benefit to the employee/irregular benefit to the client/loss to SBICAPS.
- Cyber frauds i.e. "unlawful/criminal activity that uses a computer either as an instrumentality, target or a tool for perpetuating further crimes."
- Any other type of fraud not coming under the specific heads as above.

These are frauds perpetrated by those internal to the organisation. Businesses are also susceptible to fraud committed by outsiders, such as corporate identity theft, breach of contract by vendors, intellectual property fraud or cyber-crime.

CYBER FRAUDS:

Cyber frauds are unlawful/criminal activity that uses a computer either as an instrumentality, target, or a tool for perpetuating further crimes that would include the following:

- Communication in furtherance of criminal conspiracy
- Information piracy and forgery
- Electronic Money Laundering
- Illegal Interception of Information
- Hacking
- Altering Websites
- Data theft or leakage of data to unauthorised entity.

7. Preventive measures:

Each Business Unit / Group such as Accounts Dept. , IT Dept., Treasury & Investment Dept., Administration Dept., HR Dept., C&RM Dept., PASF Group, ECM Group and DCM Group shall have the ownership for initiating necessary preventive/corrective steps in their respective areas based on the analysis/ remarks/observations from various units/audits namely, Internal Audit, Statutory Audit, Compliance Audit, CAG Audit, SEBI Inspection Report and Guidelines from time to time; as also from client feedback or complaints in order to mitigate internal and external susceptibility to fraud. The IT Department is required to make process changes in the system and technological interventions to modify / strengthen the existing systems in coordination with respective business / other Groups.

As part of preventative measures against fraud risk, surveys / assessments are proposed to be conducted on a periodic basis to assess the culture, attitude, and awareness amongst employees / external vendors and contractors about their knowledge of and response to any issues of fraud or misconduct.

Periodic awareness and outreach sessions for employees are being carried out in the form Compliance Test, Induction for new joiners, Risk Awareness Day.

The following points should be taken into consideration as a part of awareness and training to combat fraud risk in the organization:

1. Encourage a culture of zero tolerance towards frauds.
2. Fraud awareness amongst employees and customers
3. Importance of escalation of suspicious activities
4. Annual trainings for employees
5. Code of Conduct to include declaration pertaining to the data / information security and safeguarding.
6. Periodic customer awareness emails, feedback surveys, letters
7. Customer awareness measures on website

8. Systems & Controls for prevention of frauds:

Compliance of prescribed systems, policies, procedures, guidelines, and control functions are critical to the Company in prevention of frauds. All the functionaries are required to report any deviation/ breach of guidelines of the Company. An illustrative list of areas demanding focused attention of all the functionaries in Corporate Office and Regional Offices / branches, at every level, to ensure prevention of frauds, is given below:

- Sourcing of business /new connections: DOP should be adhered to, KYC norms to be strictly followed.
- Introduction of New Products/Processes/Policies: At the time of introduction of new products/policies/processes, inherent fraud risk considerations should be evaluated and documented along with adequate mitigants and processes for deviation management and monitoring thereof.
- Delegation of powers: Financial powers to sanction any payment should be as per the Delegation of powers approved by the Board. As regards IT, the capability levels permitted to officials in the system should not exceed the powers delegated to them.
- Maintaining secrecy of password is every individual's responsibility.
- Reconciliation of System Suspense Account(s) on a regular basis should be ensured.
- Job rotation should be ensured in critical roles.
- Whistle Blowing concept should be promoted/ encouraged as highlighted in the Whistleblower Policy
- Investment policy should be complied with, and any breach should be reported to the designated authority as per the policy.
- Accounting manual should be complied with and should lay down procedures for prevention of misappropriation of funds/ fraud.
- Third party dealer/supplier/builder must be contacted independently to verify genuineness of their offer/transaction.
- DLP solution to be put in place to prevent data fraud.

The above are only illustrative measures, and all the officials must take necessary steps to prevent fraud and protect the assets of the company.

9. Detection of fraud:

Some of the sources of unearthing frauds could be:

- Various audits/ inspections both by internal and external agencies
- Prompt reconciliation of inter-office accounts
- Bank Reconciliation Statement
- Electronic/print media/other outside sources
- Anonymous/pseudonymous complaints with verifiable facts
- Complaints from clients / alerts from other investigating agencies
- Any internal complaints / whistle blower allegations

- Cash shortages not reported on the date of occurrence by the person(s) handling cash, shall be reported as a fraud.
- DLP solution to detect data fraud.

10. Fraud Response System:

On detection of fraud, the department/party concerned will report to the CRO & P&COO within two working days in the format given in **Annexure - I**.

All cases of fraudulent nature must be referred to the CRO & P&COO for investigation. The P&COO will appoint an officer not below the rank of SVP or a team of officers (one of whom should be at the rank of SVP or above) to investigate the matter within a stipulated time frame. The officer/ team of officers appointed, shall have the access to all the business / operating units, relevant systems, and the authority to seek information and conduct interviews with any of the employees of the entity for the purpose of carrying their investigations and reviews. The officer/team shall also be responsible for measuring the amount of fraud loss exposure to the organization. Post investigation, the matter will be discussed/ analyzed at length and shall be put up to P&COO and MD&CEO for necessary action.

A suitable communication will be sent to all the Groups with a view to alerting them against perpetration of similar fraud. Further based on the outcomes of the investigation, the P&COO may proactively suggest enhancements to various systems and controls to remove the gaps if any, and to strengthen the internal control framework of the organization.

11. Staff accountability:

Staff are encouraged to proactively report fraudulent activity to the management. Any involvement of insiders in respect of fraud will be dealt with expeditiously. In cases involving senior executives of the organization, the Board may initiate the process of determining staff accountability.

12. Reporting requirements:

All the cases of fraud should be reported to the Audit Committee. If the financial implication exceeds Rs. 1 Crore it should be also reported to the Risk Management Committee of the Board and to the Board of Directors.

Additionally, following Monthly Reporting will be undertaken:

a. Confirmation by all respective group and functions heads for any frauds reported to Chief Risk Officer (CRO)
b. Submission of Return to SBI in FMR format as requested by SBI as per the requirement of RBI circular on Fraud Classification and Reporting

13. Review of Policy:

The Policy shall be reviewed as and when considered necessary, but at least once in two years. Changes to policy should be collated at management level and subsequently presented to the Board of Directors for approval.

14. Record Retention:

Records of fraud related matters must be retained in accordance with the Record Management Policy of the organization.

Annexure - I

Format for Reporting of fraud		
1	Department	
2	Nature of fraud like Income related payment related etc.	
3	Perpetrators of fraud internal/external/unknown	
4	Date fraud or suspected fraud discovered	
5	Actual, suspected, or attempted fraud	
6	Cause of fraud like absence of controls/failure to observe controls/unknown	
7	Brief outline of case	
8	How was fraud discovered like whistle blower/internal audit/other means	
9	Amount of loss	
10	Action taken	
11	Reported by (Name and designation and Signature)	