



**CANARA HSBC LIFE INSURANCE COMPANY LIMITED  
CIN: L66010DL2007PLC248825**

**Anti-Fraud Policy**

**Owned by:**

**Risk Management- Fraud Management Unit**

**Version no.: 2.5**

**Release Date: 9<sup>th</sup> February 2026**

**Version History**

<b>Release Date</b>	<b>Version</b>	<b>Owner</b>	<b>Revision Description</b>	<b>Approved By</b>
08/05/2013	1.0	Risk	Initial version	Board/BRC
29/07/2013	1.1	Risk	No Change	Board/BRC
August 2014	1.2	Risk	Review	Board/BRC
11.08.2015	1.3	Risk	Changes in-line with Companies Act & Insurance law, 2015 fraud related requirements	Board/BRC
09/08/2016	1.4	Risk	Minor Changes	Board/BRC
09/08/2017	1.5	Risk	Minor Changes	RMC/ Board
23/07/2018	1.6	Risk	Minor Changes	RMC/ Board
14/08/2019	1.7	Risk	Minor Changes	RMC/ Board
12/08/2020	1.8	Risk	Minor Changes	RMC/ Board
23/07/2021	1.9	Risk	Enrichment of Roles & Responsibilities of key stakeholders	RMC/ Board
02/09/2022	2.0	Risk	Minor Changes	RMC/ Board
16/08/2023	2.1	Risk	Minor Changes	RMC

28/08/2023	2.1	Risk	Minor Changes	Board
22/07/2024	2.2	Risk	Minor Changes	RMC/Board
04/03/2025	2.3	Risk	Minor Changes	RMC
26/03/2025	2.3	Risk	Minor Changes	Board
21/07/2025	2.4	Risk	Minor Changes	RMC/ Board
09/02/2026	2.5	Risk-FMU	Alignment with IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025	RMC/ Board

## Table of Contents

1.	Purpose .....	4
2.	Definitions .....	4
3.	Classification of insurance frauds.....	6
4.	Scope of application .....	9
5.	Policy objectives .....	10
6.	Ownership .....	10
7.	Compliance / Exception management .....	10
8.	Application .....	10
8.1	Fraud risk management principles.....	10
8.2	Governance.....	11
9.	Policy requirements .....	16
10.	Authorization and Review .....	22

## 1. Purpose

Fraud poses major risks to all segments of the financial sector. Fraud in insurance sector, not only reduces consumer and shareholder confidence, it can severely impact the reputation of the Company and also of the insurance sector as a whole.

Fraud events have become complex and sophisticated over a period of time, because of which, the Company is required to adopt a long term and holistic view on fraud risk management and also adopt a comprehensive framework to mitigate fraud risk.

Further, relevant laws governing Aadhaar authentication interalia, require the Company to implement reasonable safeguards towards preventing any authentication related fraud as well as those involving Aadhaar data which the Company might collect from its Customers or its employees for a defined purpose as permitted under the applicable laws.

The Company has a governance structure in place that fosters a culture of ownership and accountability at all levels of management. It has also adopted a set of values that ensure a culture where all employees understand the importance of these values and practice these values in their day to day working. This, not only, contributes to value creation for both customers as well as the shareholders but also helps in creating a stable risk environment.

This Anti-Fraud policy of Canara HSBC Life Insurance Company Ltd. (the Company) prescribes minimum standards and requirements that the Company must adopt, in order to implement an effective fraud risk management framework, in-line with the regulatory directives and Company's risk appetite. In case of any fraud noted with respect to Aadhaar data / authentication related requests, applicable requirements outlined in this policy as well as those captured in Company's Information and Cyber Security policy shall apply

This policy shall be read in conjunction with 'insurance fraud monitoring framework' prescribed by IRDAI and other relevant and applicable Company policies. The Company's Risk policy shall be the overarching guiding policy for this Anti-Fraud policy while other policies like Whistleblower Policy, Standards of Business Conduct, and Gift Entertainment and Anti-Bribery policy shall cater to the applicable/ relevant requirements specified under this Anti-Fraud policy.

## 2. Definitions

- ❖ *"Insurance Fraud" (hereinafter referred to as 'Fraud') shall mean an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to:*

- Misappropriating funds;
  - Deliberately misrepresenting/concealing/not disclosing one or more material facts relevant to *any decision / transaction, financial or otherwise*
  - Abusing responsibility, position of trust or a fiduciary relationship.
- ❖ “Aadhaar Number” means an Identification Number issued to an individual by UIDAI - An Aadhaar number, in physical or electronic form subject to Authentication and other conditions, as may be specified by regulations, may be accepted as proof of identity of the Aadhaar number holder
  - ❖ “Aadhaar Number Holder” means an Individual who has been issued an Aadhaar number under this Act
  - ❖ “Authentication” means the process by which the Aadhaar Number along with Demographic Information or Biometric Information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;
  - ❖ “Authentication record” means the record of the time of Authentication and Identity of the Requesting Entity and the response provided by the Authority thereto
  - ❖ “Authentication Facility” means the facility provided by the Authority for verifying the Identity Information of an Aadhaar number holder through the process of Authentication, by providing a Yes/ No response or e-KYC data, as applicable;
  - ❖ “Authority” / “UIDAI” means the Unique Identification Authority of India
  - ❖ “Biometric Information” means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations
  - ❖ “Core Biometric Information” means finger print, Iris scan, or such other biological attribute of an individual as may be specified by regulations
  - ❖ "Company" -means Canara HSBC Life Insurance Company Limited.
  - ❖ "Intermediary" or "insurance intermediary" includes insurance brokers, re-insurance brokers, insurance consultants, corporate agents, third party administrator, surveyors and loss assessors and such other entities, as may be notified by the Authority from time to time
  - ❖ "Insurance agent" means an individual appointed by an insurer for the purpose of soliciting or procuring insurance business including business relating to the continuance, renewal or revival of policies of insurance
  - ❖ Red Flag Indicator or RFI means a possible warning sign, that points to a potential fraud
  - ❖ Cyber or New Age Fraud means any insurance fraud carried out using digital or new age technologies.
  - ❖ **"Personal Data or Information"** means any Data or Information about an individual who is identifiable by or in relation to such Data or Information. It is any Data or Information that relates to a natural person, which, either directly or indirectly, in

combination with other Data or Information available or likely to be available with a body corporate, is capable of identifying such a person.

- ✓ **“Sensitive Personal Data or Information”** means such Personal Data or Information which consist of Information relating to:
  - ❖ Password
  - ❖ Financial Information such as Bank account or credit card or debit card or other payment instrument details.
  - ❖ Physical, physiological and mental health condition.
  - ❖ Sexual orientation.
  - ❖ Facial and Biometric Information.
  - ❖ Call Data record.
  - ❖ Medical records and history.
  - ❖ Any detail relating to the above as provided for providing service.
- ✓ **"Other Personal Information"** - Any Personal Information which is not considered Sensitive Personal Data or Information as per the above categorization will be treated as Other Personal Information.

### 3. Classification of insurance frauds

Classification of insurance frauds must be read in conjunction with the above mentioned definition of fraud. Based on the external and internal threats faced by the Company, frauds shall be classified into the following broad level categories:

- **Policyholder Fraud and/or Claims Fraud:**

This covers fraud against the insurer during the overall life cycle of the policy post policy issuance, servicing and claims processing. This category of frauds includes the following among other events:

- Fraudulent/ false death claims
- Staging of death
- Buying an insurance policy in the name of a dead / fictitious person
- Benefit payout encashment/ Surrender/ Partial Withdrawal/ Loan fraud
- Cheque fraud
- Online/Digital fraud (e.g. phishing, hacking etc.)
- Assignment Fraud
- Material non-disclosure / Misrepresentation of facts
- Forging of documents

- **Distribution Channel Fraud**

Fraud perpetuated by an insurance agent/ Insurance intermediary against the Company and/or policyholders. This category of fraud includes the following among other events:

- Premium diversion / misappropriation –Agents, Intermediary takes the premium from the customer either new business or renewal or top up and does not pass it to the Company or inflates the premium amount to the Customer passing on the correct amount of premium to the Company and keeping the difference amount with himself
- Producing false/ fabricated/ inflated bills/ invoices against services provided
- Benefit payout encashment/ Surrender/ Partial Withdrawal/ Loan fraud
- Producing false/ fabricated documents to seek business benefits from the Company e.g. awarding of contracts etc.
- Credit card/ banking fraud by vendor (e.g. agents, intermediary staff misuses credit card/ banking data available for the policyholders)
- Cheque/ instrument fraud
- Misappropriation of Funds (Removing money from customer/ policyholder accounts)
- Other instances of misdemeanor eg. Claim investigator soliciting for bribe to facilitate claim payout
- Signature forgery
- Capturing incorrect contact number in proposal forms and policy documents and subsequently answering Pre Issuance Validation Call done by the Company
- Document tampering/ forgery
- Data theft/Unauthorized use of restricted and highly restricted information including Aadhaar data with a malafide intent
- Permitting special prices or privileges to customers
- Unauthorized falsification and fabrication of Company's documents including but not limiting to any acts of fabrication done using Company's stationary or logo or pertaining to policy related information
- Act of impersonation including but not limiting to
  - Capturing of incorrect contact number in proposal forms and policy documents wherein it was proven that Pre Issuance Validation Call done by the Company was incorrectly answered by the Insurance intermediary/ agent
  - Opening of bank accounts in the name of Customer or facilitating fraudulent medicals

This category of fraud shall exclude cases of mis-selling/ sales conduct at the time of sourcing of new business. However, a case of mis-selling/ sales conduct when accompanied with any act of impersonation, signature forgery, written misrepresentation given and/ or document tampering or financial irregularities noted at the time of sale and detected post issuance of insurance policy shall be classified as fraud.

- **Internal Fraud:**

Fraud/ mis-appropriation against the Company by any of its internal staff member including employees and / or senior management (by whatever name called). This category of fraud includes, but not limited to:

- Premium diversion or misappropriation – Staff takes the premium from the customer and doesn't pass it on to the Company or inflates the premium amount to the Customer passing on the correct amount of premium to the Company and keeping the difference amount with himself
- Fraudulent financial or non-financial reporting
- Cheque or Instrument fraud / Stealing cheques
- Submission of fraudulent / forged bills for reimbursement of expenses (Travel and other Expenses reimbursements)
- Submitting false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
- Permitting special prices or privileges to customers, or granting business to favored suppliers, for kickbacks/favors
- Forging signatures
- Act of impersonation including but not limiting to
  - Capturing of incorrect contact number in proposal forms and policy documents & wherein it was proven that Pre Issuance Validation Call done by the Company was incorrectly answered by the staff
  - Opening of bank accounts in the name of Customer or facilitating fraudulent medicals
- Capturing incorrect contact number / co-ordinates in proposal forms and policy documents and subsequently interacting on behalf of/ as Customer
- Removing money from customer/ policyholder accounts
- Falsifying documents
- Selling Company's assets at below their true value in return for payment
- Misappropriation of Funds
- Benefit payout encashment/ Surrender/ Partial Withdrawal/ Loan fraud
- Data theft/Unauthorized use of restricted and highly restricted information including Aadhaar data with a malafide intent
- Aadhaar authentication related fraud
- Unauthorized falsification and fabrication of Company's documents including but not limiting to any acts of fabrication done using Company's stationary or logo or pertaining to policy related information

- **External Fraud:**

Fraud perpetrated by external parties' / service providers / vendors etc. against the Company and/or policyholders. This category of fraud includes, but not limited to:

- Data theft/Unauthorized use of internal, restricted or Confidential information with a malafide intent
- Unauthorized falsification and fabrication of Company's documents including but not limiting to any acts of fabrication done using Company's stationary or logo or pertaining to policy related information
- Submission of fraudulent / forged bills with or without collusion with internal staff members
- Submission of fake reports or suppression of any material facts or evidence

- **Complex affinity Fraud:**

Fraud orchestrated against the Company and/or policyholders. involving collusion among one or more fraud perpetrators in the above categories. Such frauds include but are not limited to the following

- Collusion amongst Sales Support staff and Hub Operations staff to orchestrate a fraud to against the Company or its Customer's
- Collusion of Policyholder with hospitals or third-party administrators to submit fake claims
- Involvement of a cartel in issuance of policies of potentially vulnerable section of the society for the purpose of claiming Insurance benefits by colluding with other stakeholders of the society

For the purpose of this policy, the same shall exclude any instances of suspected fraud before policy issuance where eventually the proposal gets rejected.

There could be more scenarios or combination of scenarios that might be considered under the definition of fraud and those might fall into any of the above categories. Functions/ process owners are advised to seek assistance from Risk management function over such matters.

#### **4. Scope of application**

This Anti-Fraud policy is applicable to all employees (including Insurance Intermediaries and agents/ vendor/ contractual resources working on/ supporting Company's processes) and Directors of the Board of the Company, and requires implementation by all functional areas within the Company. This shall also include cases of fraud noted from its Insurance self-networking platform (ISNP) and the process outlined below shall apply for such cases as well.

Additionally, the Company, in due course of its business, is required to interact on account of seeking services or providing services as applicable, with external entities like vendors, counterparties, intermediaries, partner banks, Insurance Intermediaries and agents and customers/ policyholders on which the relevant extracts of the policy shall prevail.

## **5. Policy objectives**

Anti-Fraud policy has been established in order for the Company to deliver on following objectives

- Identify, assess and minimize the risk of fraud thereby protecting and further strengthening of customers as well as shareholders confidence
- Implementing controls that would help in deter, prevention, early detection, reporting, and investigation of fraud events
- Creating and maintaining a culture of honesty and high ethics by ensuring adequate awareness amongst the Company's staff, partner bank staff, Insurance Intermediaries and agents, vendors and customers towards importance of fraud risk management
- Complying with relevant and applicable regulatory directives/ guidelines

## **6. Ownership**

This Policy is owned by the Risk Management- Fraud Risk team and is approved by the Risk Management Committee and the Board of Directors.

## **7. Compliance / Exception management**

Any exception to the Policy application or fraud events noted must be escalated to Chief Risk Officer and relevant department head for appropriate action.

## **8. Application**

### **8.1 Fraud risk management principles**

The following principles shall apply to the management of fraud risk across the Company:

- The Company believes in honesty and fairness while discharging all its internal as well as external commitments and expects the same from all its internal and external stakeholders, staff, vendors and customers
- The Company believes in having transparent, smooth and well controlled processes to enhance its value proposition to its customers as well as shareholders
- Fraud risk management is the responsibility of every staff member including Company's Senior management ,Board of directors and other persons/ entities covered under the policy

- A consistent framework shall be applied across the Company to facilitate the prevention, early identification/ detection, assessment, management and reporting of fraud risk events
- Investigation of fraud risk events shall follow an un-biased and neutral approach
- Appropriate disciplinary actions shall be taken against individuals found involved in fraud events in line with Company's disciplinary action policy.

## **8.2 Governance**

It is important that fraud risk management is closely linked in with the business strategy and that all anti-fraud activity supports rather than hinders it. In line with Company's Risk Policy and the decentralized approach adopted by the Company towards risk management, day to day responsibility of adopting and following fraud risk management practices shall continue to remain at the functional level.

Risk management function, being a function independent of business operations shall also adopt the role of fraud risk management and in conjunction with first line of defense shall prescribe suitable fraud risk management framework, standards, guidelines and controls that would need to be followed and embedded in relevant functions and processes. The function shall also be responsible for provision of advice to support implementation of this Policy. All actual/ established fraud events shall be reported to relevant governance forums basis defined thresholds/ materiality

**Board and Risk Management Committee (RMC)** shall be responsible for ensuring the following

- Reviewing and approving the Anti-Fraud policy
- An effective Anti-Fraud policy and framework is implemented.
- Maintaining an oversight on the Company's Anti-fraud framework and related incidents noted basis the reporting requirement agreed and events notified via the Fraud Monitoring Report to IRDAI
- Quarterly update on frauds of serious nature and with amounts wherein the exposure exceeds rupees one crore.

### **Fraud Monitoring Committee (FMC)**

The Fraud Monitoring Committee (FMC) shall be headed by the Chief Risk Officer **and** include Senior representatives from relevant departments, such as Underwriting, Claims, Legal or any other department as deemed necessary.

The Committee shall be responsible for implementing and maintaining the Fraud Risk Management Framework within the Company. The Committee shall oversee all relevant activities to ensure robust mechanisms for fraud deterrence, prevention, detection, reporting, and remediation. FMC is responsible for periodically reviewing fraud risk exposures, monitoring compliance with established controls, and recommending corrective actions to strengthen the framework and safeguard organizational integrity.

The FMC shall report to the Board level Risk Management Committee (RMC).

### **Functions of the Fraud Management Committee (FMC)**

The Fraud Management Committee shall perform the following functions:

- **Maintain an oversight on the fraud incidents noted towards ensuring** timely and effective responses to suspected or confirmed instances of fraud.
- Recommend appropriate measures for fraud risk management and ensure periodic updates based on experience and emerging risks.
- Facilitate coordination with industry bodies, law enforcement agencies, and regulatory authorities to pursue fraud cases and share intelligence on known schemes and perpetrators.
- Facilitate submission of quarterly reports to the Risk Management Committee outlining its activities, observations, recommendations, and the financial impact of fraud on the insurer.
- Maintain an oversight on the fraud risk assessment exercise undertaken by Fraud Monitoring unit. Facilitate submission of the Annual Fraud Risk Assessment report to the Board of Directors through the RMC.
- Facilitate reporting of all internal fraud cases to the Audit Committee, in addition to the RMC.

### **Fraud Risk team / Fraud Monitoring Unit (FMU)**

The fraud risk team / FMU within **Risk Management function** shall support the Fraud Monitoring Committee (FMC) in fulfilling its obligations. It will ensure effective execution of measures recommended by the FMC and assist in strengthening the organization's **Fraud risk** management framework.

**The Fraud Risk team / Fraud monitoring unit** shall be responsible for the following:

- Establishing fraud risk management framework including relevant policies and procedures in the Company as per the requirements laid down in this Policy
- Conduct an annual fraud risk assessment to identify potential vulnerabilities across business lines and activities, leveraging historical data, emerging trends, and Red Flag Indicators (RFIs).
- Have access to all fraud events being reported via Whistleblower ID
- Responsible for central recording, collation, management and usage of relevant data and trends to support the fraud risk management process. Maintain records of all fraud-related incidents for analysis and reporting purposes.
- Creating awareness among employees/ intermediaries and Insurance agents/ policyholders to counter insurance and related frauds
- Escalate and report fraud events to management or Board as per the established thresholds
- Undertake investigations of alleged or suspected fraud cases basis the scope outlined
- Support Legal function towards liaising and co-ordination with law enforcement agencies for designated fraud cases
- Facilitate coordination with industry bodies, law enforcement agencies, and regulatory authorities to pursue fraud cases and share intelligence on known schemes and perpetrators.

- Work along with Life council/ IIB towards having a structure for exchange of necessary information on frauds amongst other insurers. Furnishing various reports on frauds established to the Regulator as stipulated in this regard.
- Furnish periodic reports to Fraud Monitoring Committee and Risk Management committee for cases that meet its reporting criteria
- Recommend appropriate measures for fraud risk management and ensure periodic updates based on experience and emerging risks.
- Identify areas for enhancement and ensure ongoing adaptation of the Fraud Risk Management Framework to address evolving risks.
- Preparing fraud monitoring report (FMR) 1 as per IRDAI format within 30 days of close of the financial year.

**Respective functions/ departments and Business risk and control managers (BRCM)** act as a part of first line of defense shall be responsible for the following

- Implementing preventive and early detective controls as specified by Risk Management- Fraud risk team / Fraud Management Unit and those prevalent as per accepted best practices and adopt these controls in day to day activities
- In line with the structure outlined, relevant teams to ensure participation, sharing of information and collaboration with industry members in area of fraud. Further involving Risk management- Fraud risk team/ Fraud Management Unit in design review of new processes, that the function owners believes may be vulnerable to frauds, or wherever such processes are undergoing any material/ significant changes
- Providing all support during conduct of investigations on fraud related matters to Risk management - Fraud risk team/ Fraud Management Unit
- Notifying and reporting instances of fraud to the Risk Management- Fraud risk team/ Fraud Management Unit
- Assist Risk Management - Fraud risk team / Fraud Management Unit during risk assessment for their area
- Documenting anti-fraud controls as a part of their SOP and functional risk control self-assessment document and periodic testing of the same
- Based on business operations, historical experience, emerging trends, and other relevant factors, identify/ monitor applicable RFIs for fraud detection and incorporate them into operational workflows in their day-to-day business dealings and consequent action thereupon. Conduct periodic reviews of RFIs to ensure they remain relevant and effective in detecting potential fraud.
- Maintenance of Caution repository encompassing Company staff, distribution channels, hospitals, third party vendors and other perpetrators of fraud

- Periodic training/ updating underlying logics for fraud detection models in use. Ensuring IIB Quest database is kept updated at all times by relevant teams
- Ensuring any data shared is strictly basis job role & business need. Any channel conflict should be avoided at all costs
- Ensuring availability of records as required by applicable guidelines including but not limiting to call recordings, medical & policy records
- Towards ensuring due diligence is carried out on entities and individuals prior to entering into any agreements or their appointment

**Sales Governance & Training and Digital SBU:**

- Maintaining an oversight on Company's Sales Quality parameters
- Ensuring new business and renewal premium payments are made by the bonafide policyholder only using means as approved by the Company
- Channel conflict during policy login & issuance is avoided and dealt in line with the stated procedures
- Ensuring requisite due diligence is carried while logging of proposals in avoiding any anti selection risk or willful non-disclosure of material facts
- Carrying periodic reinforcements on vulnerable areas noted basis fraudulent events noted and general anti-fraud guidelines

**HR-Learning & Development, Marketing and Sales training:**

- Devising a mechanism towards annual reading of Company's Anti-fraud policy and ensuring compliance to the same by all employees
- Ensuring key themes and aspects from Fraud risk area are covered in Induction programs and Sales training programs and in Marketing initiatives for internal and external Customers as applicable
- Maintaining relevant records pertaining to Training & awareness

**Legal function:**

- Providing advisory support in identified fraud cases basis investigation reports, findings and other documentary evidences available;
- Providing assistance in dealing with law enforcement agencies and towards initiation and conduct of recovery or prosecution measures before Judicial/Quasi-judicial authorities in fraudulent cases involving significant financial and/or reputation loss or Customer impact
- Compliance with Company's Anti-fraud Policy and its Zero tolerance to fraud should be outlined in the agreements/ or their appointment letter

**Compliance function:**

- Submission of fraud monitoring report (FMR) report with the regulator as well as general liaisoning with the Authority

**Internal audit function:**

- Internal audit function, from time to time as a part of their approved internal audit plan, shall carry out fraud-sensitive audits for compliance with the Fraud Risk Monitoring Framework and ascertain the adequacy, efficiency and operating effectiveness of anti-fraud controls deployed within the Company and provide independent assurance to the Audit Committee.

**All employees are** responsible for the following

- Follow the requirements as outlined in this policy and also aspects mentioned as a part of their code of conduct and joining documents
- Not indulge in fraudulent activities that may cause harm to the Company or its Customers
- Reporting of any control weaknesses or fraudulent events to the Company via available touch-points
- Avoid / deter any financial relationship with fellow employees/ Customer's/ business partners/ Insurance Intermediaries and agents/ designated third parties/ any other business entities. Proactively disclose any such relationships as applicable to BHR
- Upon joining, the employee is obligated to provide truthful and accurate information as requested. Additionally, the employee must promptly notify the Company of any ongoing civil or criminal legal proceedings involving himself throughout their employment with the Company

**Insurance Intermediary and Agents / Partner bank staff** shall be responsible for the following:

- Adopting high standards of conduct while doing business for the Company in accordance with the rules and regulations
- Not indulge in fraudulent activities that may cause harm to the Company or its Customers
- Reporting of any fraudulent events to the Company via available touch-points
- Follow the requirements mandated by the regulation as well as those outlined in this policy, their contracts / aspects mentioned as a part of their onboarding documents
- Avoiding channel conflict at all times

The Company carries out periodic awareness initiatives in conjunction with Marketing, Internal Communication and Sales training teams to ensure its Customer/ policyholders as well as staff are sensitized on areas pertaining to fraud risk and ensure requisite awareness therein to prevent and avoid any negative Customer outcome to the extent possible. The Customers are apprised of our guiding principles with respect to being honest, open and consistent in our communications.

The Board and RMC shall review this Anti-Fraud policy at least on an annual basis or at such other intervals as it may be considered necessary

## **9. Policy requirements**

The Company works on the principle of “utmost good faith” and requires honesty and fairness to be followed at all times during all its internal as well as external engagements. As a part of fraud risk management framework, it is the responsibility of management at all levels including that of Company’s Board, to ensure that effective internal control systems are in place and operating to minimize the potential for fraud at all times.

The Company is committed towards ensuring that opportunities of fraud are reduced by the effective operation of the control, governance and accounting systems and supported by its organizational procedures at all levels.

In order to ensure that requisite Anti-fraud controls are in place towards prevention and detection of fraudulent events, the Company shall ensure compliance with requirements stipulated in this policy towards security of Aadhaar/ E-KYC infrastructure as well as those mentioned in Company’s Information and Cyber Security policy.

In order to create an effective fraud risk management framework in the Company, Anti-Fraud policy prescribes/ requires the following:

### **a) Creation and sustenance of an effective antifraud environment**

- Fraud risk management framework shall be established in the Company along with other relevant policies and procedures supporting such framework e.g. Conflicts of Interest Policy, Standards of Business Conduct, Gift Entertainment and Anti Bribery Policy, Procurement Policy, Whistleblower Policy and other such relevant policies and procedures as required under regulations or Corporate Governance guidelines
- Fraud risk management framework shall be implemented and adopted at all functional levels of the Company and shall adequately cater to all the three categories of fraud as specified earlier in this policy
- Ongoing employee and management awareness shall be carried out on Anti-Fraud policy, supporting policies and procedures

### **b) Fraud risk assessment:**

The Company shall conduct an Annual Fraud Risk Assessment exercise to identify potential vulnerabilities across business lines and processes impacting Company’s fraud risk landscape using past experiences, emerging trends and identified Red Flag Indicators (RFIs),

The Company shall ensure that relevant red flags Indicators (RFIs)/ early warning indicators are documented in areas vulnerable to fraud. Such RFIs shall be periodically reviewed for their continued relevance and effectiveness in detecting fraud.

**c) Cyber of New age fraud:**

**in order to** effectively prevent and mitigate cyber-related or emerging fraud risks, the Company shall adopt multiple measures not limiting to the following:

- Establish and implement an Information & Cybersecurity framework designed to safeguard against evolving cyber threats and fraud schemes.
- Regularly monitor and strengthen fraud risk management systems and processes, including incident tracking databases, customer identity verification mechanisms, and access control measures.

**d) Caution repository:**

The Company shall ensure that relevant BRCM's as applicable maintain a Caution repository encompassing Company staff, distribution channels, hospitals, third party vendors found in indulgence of fraud.

**e) Adoption of controls for prevention and early detection of fraud events**

Fraud Prevention is a key part of the fraud risk management process and effective implementation of preventive controls shall protect the Company from financial loss and reputational damage.

Fraud prevention requires an innovative, broad approach and includes staff, agents and customer awareness, protection of information, trend and modus operandi analysis, intelligence gathering, risk assessment, data analytics and involvement in business systems and process designs to remove fraud risk related vulnerabilities at an early stage. Key requirements under fraud prevention and early detection are specified below:

- Risk assessments in applicable areas basis experience to identify vulnerabilities and control weaknesses

Building of relevant red flags Indicators (RFIs) early warning indicators in areas vulnerable to fraud, implementation of preventive as well as early detective controls, either automated or manual depending upon the level of risk exposure, in areas that are vulnerable to fraudThe Company shall provide means/ channels of communicating/ reporting of fraudulent events e.g. through designated email id of fraud risk team/ Fraud Management Unit, whistleblower ID etc. as it deems necessaryTypically preventive controls in such areas include but not limited to:

- Effective segregation of duties,job roles and ensuring role-based access control.
- Maker-checker controls in applicable processes

- Customer identification and verification procedures followed before divulging sensitive customer details
- Performing pre-employment screening of staff, due diligence of critical vendors/ outsource partners before short listing basis risk exposure
- Performing relevant checks before issuing a policy to the customer or before making a payout including death or maturity payout to customers/ policyholders
- Job rotation as deemed necessary for select management and staff in fraud sensitive positions
- Prescribing anti-fraud controls through contractual provisions with select vendors basis risk perceived
- Establishing early fraud warning signals through the use of risk indicators and any adverse trends emanating basis fraud events noted
- Customer awareness on conventional and emerging fraud events/ trends. Staff and senior management awareness and training on fraud risk management
- Exchange information as deemed necessary with respect to fraud events specifically with respect to policyholders/ claims fraud amongst all insurers through life council/IIB
- Ensuring that employment contracts are having suitable terms mandating employees to safeguard Sensitive Personal Data and information collected as required by Digital Personal Data Protection Act 2023, Information and Cyber Security Guidelines prescribed by IRDAI and applicable provisions of Information Technology Act, 2000 and also to prevent any unauthorized collection, storage, usage and dissemination of Sensitive Personal Data and/or Aadhaar data in line with the requirements stipulated under the relevant laws
- Use of tools and models to help Company mitigate fraud risk to the extent possible
- Validating the identity of the prospect during logging of fresh business proposals as well as Customers before processing of any Policy Servicing request

With respect to Aadhaar data and EKYC process and to prevent authentication related frauds the preventive measures shall include but not limit to the following

- Masking of Aadhaar data as required by regulations
- No biometric or OTP information is stored with the Company
- Aadhaar number is stored encrypted in Aadhaar vault only and accessible to designated staff strictly only on a need to know basis
- Certified biometric devices shall be used
- Aadhaar Authentication requests are digitally signed
- Terminal devices used shall ensure users are authenticated and devices protected
- Further terminal details shall be suitably captured
- The "PID Block" (Personal identity) shall be kept encrypted including channel for transmitting the same

Detective fraud controls include but not limited to:

- Carrying out onsite vendor audits for designated vendors wherein fraud risk exposure is high / which are responsible for execution of such controls
- Review of work allocation to vendors to minimize the possibility of vendor favoritism in applicable areas
- Mystery shopping activity or seeding exercises
- System event and activity log monitoring
- Provide communication channels and mechanisms, specified through this policy as well as in the whistleblower policy, for relevant stakeholders including staff members, senior management, Board of directors, customers, partner bank staff, Insurance agents and customers to report matters pertaining to fraud
- Regular reviews carried out by the internal audit function to identify fraud events that may not get reported or identified in the normal course of business
- Usage of anti-fraud solutions as envisaged and implemented by the Company from time to time
- Use of tools and models to help Company detect and mitigate fraud risk to the extent possible
- Periodic monitoring and reporting of early claim experience with channel partners, agency head and Sales team and addressing of any systemic issues noted

With respect to Aadhaar data and EKYC process and to prevent authentication related frauds the detective measures shall include but not limit to the following

- Authentication and transaction logs captured requisite details as required by the regulation
- Such logs will be retained for a minimum specified period with controlled access

The above mentioned controls must be considered and adopted by functions wherever necessary with guidance from the Risk Management- Fraud risk team/ Fraud Management Unit.

**f) Establishment of procedures for fraud monitoring, investigation and reporting**

- All customers, intermediaries, Insurance agents, managers and staff must report if they have any knowledge or suspicion of fraud to either
  - ✓ Their line manager
  - ✓ Risk Management- Fraud risk team /Fraud Management Unit
  - ✓ Whistleblower ID
  - ✓ Complaints redressal unit
  - ✓ Sales governance team
- As soon as the complainants or communication from witnesses of alleged misconduct including whistle-blowers is received by the fraud risk team/ Fraud Management Unit, a preliminary evaluation of the misconduct would be initiated. This step is essential for preserving information that could be crucial for further investigation or resolution. Basis the merits of the case a call

might be taken to suspend the employee concerned or restrict their access to Company/ Bank premises or terminate the agency license

- Any fraudulent event noted involving Aadhaar data / authentication related request shall be duly investigated and dealt in line with applicable provisions outlined
- The Company shall conduct periodic awareness sessions on fraud risk management, both for its internal as well as external stakeholders to ensure adequate awareness on Company's Anti-Fraud policy and related requirements
- Company shall establish investigation protocols and process for alleged or suspected fraud cases or any non-compliance to this policy. All investigations must be closed in a timebound manner as outlined in Anti- Fraud SOP.
- The Company shall investigate all suspected or alleged fraud events and highlight key learning's noted including any additional preventive and detective controls to be implemented. Co-ordination with law enforcement agencies, wherever required, shall be carried out for closing fraud cases on a timely and expeditious basis
- The Company respects the privacy of its employees and Insurance agents while accessing Information assets; however the Company reserves the right towards monitoring usage of information assets allocated to employees and Insurance agents including screening of their personal assets e.g. Mobile phones, tablets etc. which might be used in day to day business dealings to check for any probable non compliances or any inappropriate usage vis-à-vis Company's policies & procedures arising out of any investigation / inquiry against the staff/ Insurance agents or to respond to legitimate requests arising out of any legal proceedings.
- Exchange of information as deemed necessary with respect to policyholders/ claims fraud amongst all/ select insurers to mitigate fraud risk
- All fraud cases shall be highlighted to respective banks by Sales Governance / Business Development teams wherever role of bank staff is under scrutiny or other inputs are required from the bank to investigate the case
- All established and applicable fraud cases wherever role of partner bank/ Insurance Intermediary staff and agents is proven shall be dealt in line with the consequence management grid agreed. Appropriate action shall be undertaken for all established cases of fraud. Any fraud involving Aadhaar related data or E-KYC Authentication facility shall be treated as a non-compliance against the Code of conduct signed by all staff and will result in necessary disciplinary action commensurate with the violation noted. Further applicable provisions prescribed in the Aadhaar law and other applicable regulations shall also apply
- Anti-fraud controls shall be periodically tested by BRCM (Business Risk and Control Management) to check its adequacy and operating effectiveness
- The Company shall establish thresholds that it deems appropriate for reporting such matters to Risk Management committee or internal committee/ committees reviewing fraud events. Principle of proportionality and nature, scale and complexity of the business and risks to which

the Company is exposed to, shall define these thresholds. The Company shall report to UIDAI in case of any material fraud noted with respect to its Authentication systems within its network as well as those involving authentication requests and Aadhaar data in general. The Company shall extend full cooperation to the Authority in case of any investigation involving Authentication related fraud(s) or dispute(s).

- The Company shall pursue with recovery efforts / legal recourse in cases involving financial loss or reputation loss or significant Customer impact basis merits of the case and recommendation from Legal team
- The Company, as per the regulatory directive, shall file fraud monitoring report (FMR) 1 and 2 with IRDAI every year within 21 days of close of the financial year providing details of the fraud cases noted for the last financial year and outstanding cases that have been closed in the prescribed format

The Company may also seek relevant and applicable insurance covers, as it deems appropriate, to safeguard its interests in case of events of fraud.

#### **g) Due Diligence**

Respective department heads and HR ( as applicable) should ensure that comprehensive due diligence is carried out on entities and individuals prior to entering into any agreements or their appointment. This process helps verify the legitimacy, integrity, general experience with peers and reliability of potential business partners and employees.

The existence of company's Anti-fraud Policy and its Zero tolerance to fraud should be explicitly mentioned in the agreement/ or their appointment letter. It should also be clearly indicated that any indulgence into said activity may result in removal/dismissal from the services. This activity reinforces the company's commitment to ethical practices and serves as a deterrent against fraudulent behavior.

#### **h) Mandatory Training & awareness:**

Mandatory periodical training on ethical conduct and fraud awareness must be carried out at all levels of staff by the fraud risk management function to ensure that requirements of the anti-fraud policy are enforced amongst all stakeholders. The following are few steps to set up such a system:

- As a part of employee/ Insurance agent induction educate new joiners via an Anti-Fraud training module on the ethical standards expected within the organization, raise awareness about various types of fraud risks that the organization may face, highlighting the Anti-Fraud Policy, including their roles and responsibilities in preventing and reporting fraud
- Conduct an annual refresher of Anti-Fraud training for all employees. As a part of the training module,

- An acknowledgement shall be built in the training module and taken from employees to confirm that they have read and understood the requirements emanating from Company's Anti-fraud policy and agree to comply with the same at all times
- Conduct periodic training sessions for BRCM's and other identified functions / areas basis risk perceived to ensure continuous awareness and reinforcement.
- Ensure Customer's are sensitized of measures to combat fraud
- Update training content periodically to include new fraud schemes, regulatory changes, and lessons learned from past incidents.
- Maintain records of training completion for designated staff to ensure compliance and for auditing purposes.

## **10. Authorization and Review**

This policy was last approved by the Board on 9<sup>th</sup> February 2026. It is reviewed on an annual basis or more frequently as required.

Any applicable regulatory changes will be considered as part of the Policy. Necessary changes to the Policy will be incorporated and presented in the next meeting of the Committee/ Board.

\*\*\*\*\*