Anti-Fraud Policy

Owned by:
Risk Management- Fraud Risk Team

Version no.: 1.8
Release Date: 12th August 2020

Version History

Release Date	Version	Owner	Revision Description	Approved By
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

Table of Contents

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 also 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 Aadhar 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 Oriental Bank of Commerce 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 & Cyber Security policy shall apply

This policy shall be read in conjunction with 'insurance fraud monitoring framework' prescribed by IRDAI in January 2013 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 & Anti-Bribery policy shall cater to the applicable/ relevant requirements specified under this Anti-Fraud policy.

2. Definitions

"Fraud" in insurance 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;

This may, for example, be achieved by means of:

- Misappropriating assets, funds;
- Deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial/ health decision;
- Abusing responsibility, a position of trust or a fiduciary relationship
- Impersonation

- "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 Oriental Bank of Commerce Life Insurance Company Limited.
- "Personal Information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.
- "Sensitive Personal Data or Information" - Sensitive Personal Data or Information of a person means such personal 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;
  - ✓ Medical records and history;
  - ✓ Aadhaar related information including Biometric 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 threats posed by external and internal agents related to the Company, frauds shall be classified into three broad level categories:

- **Policyholder Fraud /or Customers Fraud:**
  This covers fraud against the insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim. This category of frauds includes events but not limited to the following:
  - Fraudulent/ false death claims
  - Staging of deaths
  - Buying an insurance policy in the name of a dead person
  - Benefit payout encashment fraud
  - Cheque fraud
  - Online/Digital fraud (eg. phishing, hacking etc.)

- Assignment Fraud

- **Intermediary Fraud:**
  Fraud perpetuated by an insurance agent/ Corporate Agent/ intermediary/ Third Party Administrators (TPAs)/ vendors against the Company and/or policyholders. This category of fraud includes but is not limited to the following:
  - Premium diversion / misappropriation –Intermediary takes the premium from the customer either new business or renewal 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
  - 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. 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 eg. Claim investigator soliciting for bribe to facilitate claim payout
  - Signature forgery
  - Capturing incorrect contact number in proposal forms & policy documents & subsequently answering Pre Issuance Validation Call done by the Company
  - Document tampering
  - Data theft/Unauthorized use of restricted & highly restricted information including Aadhaar data with a malafide intent
  - Permitting special prices or privileges to customers

  This category of fraud shall exclude cases of mis-selling/ sales conduct at the time of sourcing of new business. However, any cases of signature forgery, written misrepresentation given at the time of sale by any intermediary and detected post issuance of insurance policy shall be classified as fraud.

- **Internal Fraud**:
  Fraud/ mis-appropriation against the Company by any of its officer or staff member (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 and non-financial reporting
  - Cheque or Instrument fraud / Stealing cheques
  - Submission of fraudulent / forged bills for reimbursement of expenses (Travel & 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
  - Capturing incorrect contact number in proposal forms & policy documents & subsequently answering Pre Issuance Validation Call done by the Company
  - Removing money from customer/ policyholder accounts
  - Falsifying documents
  - Selling Company's assets at below their true value in return for payment
  - Misappropriation of Funds
  - Data theft/Unauthorized use of restricted & highly restricted information including Aadhaar data with a malafide intent
  - Aadhaar authentication related fraud

For the purpose of this policy, the same shall exclude any instances of fraud identified 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 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 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 & minimize the risk of fraud thereby protecting and further strengthening of customers as well as shareholders confidence
- Implementing controls that would help in prevention, early detection, reporting and investigation of fraud events
- Creating & maintaining a culture of honesty & high ethics by ensuring adequate awareness amongst the Company's staff, partner bank staff, 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 & 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 function and in conjunction with first line of defense shall prescribe fraud risk management framework, standards, guidelines, controls that would need to be followed and embedded in relevant functions. 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

The Risk Management function-Fraud risk team 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
- Have direct access to all communication channels being used for reporting fraud events e.g. Whistleblower ID
- Responsible for central recording, collation, management and usage of relevant data and trends to support the fraud risk management process
- Creating awareness among employees/ intermediaries/ policyholders to counter insurance & related frauds
- Escalate and report fraud events to management or Board as per the established thresholds
- Undertake investigations of alleged or suspected fraud cases
- Support Legal function towards liaising and co-ordination with law enforcement agencies for designated fraud cases
- Establish procedures for exchange of necessary information on frauds amongst other insurers, life insurance council. This shall include participation, sharing of information & collaboration with industry members, life insurance council in this regard
- Furnishing various reports on frauds to the Regulator as stipulated in this regard
- Furnish periodic reports to Risk Management committee for cases that meet its reporting criteria

- Maintaining an oversight on adequacy of anti-fraud controls documented as a part of functional RCSA. Risk assessment for select areas basis the experience & provide guidance with respect to augmentation of anti-fraud controls

Respective functions/ departments and Business risk & control managers 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 and prevalent accepted best practices and adopt these controls in day to day activities
- Involving Risk management- Fraud risk team 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 of fraud related matters to Risk management function- Fraud risk team
- Notifying and reporting instances of fraud to the Risk Management- Fraud risk team
- Assist Risk Management - Fraud risk team during risk assessment for their area
- Documenting ant-fraud controls as a part of their SOP & functional risk control self-assessment document and periodic testing of the same Monitoring of red flags in their day to day business dealings & consequent action thereupon

Intermediary/ Partner bank staff shall be responsible for the following

- Adopting high standards of conduct while doing business for the Company
- 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

Risk Management Committee (RMC) shall be responsible for ensuring that an effective Anti-Fraud policy and framework is implemented.

In addition to being monitored at the RMC, fraud risk shall also be one of the areas of risk that would be reviewed periodically in the **Operational risk and internal control group (ORIG).**

Internal audit function, from time to time as a part of their approved internal audit plan, shall carry out reviews to ascertain the adequacy, efficiency and operating effectiveness of anti-fraud controls deployed within the Company and provide independent assurance to the Audit Committee.

The Company carries out periodic awareness initiatives to ensure its Customer/ policyholders 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.

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 to 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 posture of Aadhaar/ E-KYC infrastructure as well as those mentioned in Company's Information & Cyber Security policy.

In order to create an effective fraud risk management framework in the Company, this 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 & 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) 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 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 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 & control weaknesses
- Building of relevant red flags/ early warning indicators in areas vulnerable to fraud Implementation of preventive as well as early detection controls, either automated or manual depending upon the level of risk exposure, in areas that are vulnerable to fraud
- The Company shall provide means/ channels of communicating/ reporting of fraud events e.g. through designated email id of fraud risk function, whistleblower ID etc. as it deems necessary

Typically preventive controls in such areas include but not limited to:

- Effective segregation of duties and job roles
- Maker-checker controls
- 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 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 MIS

- 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
- Ensuring that employment contracts are having suitable `terms mandating employees to safeguard Sensitive Personal Data and information collected as required by Information & Cyber Security Guidelines prescribed by IRDAI & applicable provisions of Information Technology Act, 2000 and also to prevent any unauthorized collection, storage, usage & dissemination of Sensitive Personal Data and/or Aadhaar data in line with the requirements stipulated under the relevant laws
- Use of tools & models to help Company mitigate fraud risk to the extent possible

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

- 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 now basis
- Certified biometric devices shall be used
- Aadhaar Authentication requests are digitally signed
- Terminal devices used for the same shall ensure users are authenticated & devices protected
- Further terminal details shall be suitably captured
- The “PID Block” shall be kept encrypted including channel for transmitting the same

Detective fraud controls include but not limited to:

- Carrying out onsite vendor reviews 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 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 implemented by the Company from time to time
- Use of tools & models to help Company detect & mitigate fraud risk to the extent possible
- Periodic monitoring & reporting of early claim experience with channel partners & Sales team

With respect to Aadhaar data & 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.

c) Establishment of procedures for fraud monitoring, investigation and reporting

- All customers, intermediaries, managers and staff must report knowledge or suspicion of fraud to either
  - Their line manager
  - Risk Management- Fraud risk team
  - Whistleblower ID
  - Complaints redressal unit
  - Sales governance team
- Any fraudulent event noted involving Aadhaar data / authentication related request shall be duly investigated & dealt 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
- The Company shall investigate all suspected or alleged fraud events and highlight key learning's noted including any additional preventive & 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
- 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 team wherever role of bank staff is under scrutiny or other inputs are required from the bank to investigate the case
- All established & applicable fraud cases wherever role of partner bank staff is proven shall also be reported to sales quality subcommittee (SQSC) of respective banks for noting & necessary action
- 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 & other applicable regulations shall also apply
- Anti-fraud controls shall be periodically tested by BRCM 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 recovery/ legal recourse procedures in case of a financial loss or reputation damage
- The Company, as per the regulatory directive, shall file fraud monitoring report (FMR) 1 and 2 with IRDAI every year within 30 days of close of the financial year providing details of the fraud cases noted for the last financial year 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.

10. Authorization and Review

This policy was last approved by the Board on 14th August 2019. It is reviewed on an annual basis or more frequently as required.

*****