

# **Guidance Note on Fraud Risk Management**

# *Table of Contents*

<b>1. Purpose, objective, and applicability</b>	<b>3</b>
<b>2. Structure of ONDC network</b>	<b>3</b>
<b>3. Participants of ONDC</b>	<b>3</b>
<b>4. Life cycle of a transaction over ONDC Network</b>	<b>4</b>
<b>5. What is fraud?</b>	<b>5</b>
<b>6. Operationalization of fraud prevention controls</b>	<b>9</b>
<b>7. Roles and responsibilities of Network Participants</b>	<b>10</b>

## 1. Purpose, objective, and applicability

- 1.1 The overarching objective of fraud risk management framework is to develop an anti-fraud environment that enables to detect and prevent potential fraud as well as develop fraud mitigation strategies. The aim of fraud risk management framework is to provide Network Participants (“NP”) a network that is based on the following principles:
- Transparency, and accurate information
  - Performance assurances
  - Choice and viability
  - Fair business environment and treatment
  - Safe environment
  - Customer service and grievance redressal
- 1.2 This document shall serve as a guidance to the Network Participants on how to prevent and detect fraud in a timely manner in relation to transactions undertaken on ONDC network.

## 2. Structure of ONDC network

- 2.1 ONDC Network is a decentralized and an unbundled network. It is a network of different entities coming together to offer products or services to Buyers on one end and manage Sellers on the other end. Instead of a central entity monitoring and controlling operations, the network uses interoperability, common rules of engagement at the network-level and dynamic, digital contracts to allow Network Participants to coordinate their actions to successfully complete orders on the Network and fulfil them.

## 3. Participants of ONDC

- 3.1 ONDC network comprises of Network Participants who join ONDC as Buyer side Application, Seller side Application or Gateway coming together to form the open network. Network Participants will be from a broad spectrum of domains ranging from food and beverage, retail, logistics service providers, restaurants, hotels, etc. There are three types of Network Participants for ONDC:
- **Buyer side Applications** - Buyer side Applications are Network Participants that handle Buyer-side operations such as Buyer acquisition, search and discovery, and give functionality to the Buyer to place orders on the Network.
  - **Seller side Applications** - Seller side Applications manage seller-side operations and can be of the following two types:
    - a. **Marketplace Seller Nodes (MSNs)** - MSNs are essentially aggregators. They allow Sellers (who are not themselves network Participants) to transact on the Network. MSNs do not hold any inventory, but rather function as pure-play marketplaces.
    - b. **Inventory Seller Nodes (ISNs)** - ISNs are themselves Sellers who also are Participants in the network and own the inventory which is being sold by them.

- **Gateways** - Gateways purely function as nodes for multicasting search queries and collecting results. Thus, they play a crucial role in search and discovery.
- **Ecosystem Participant** shall mean any participant in the ONDC ecosystem, other than Network Participants, and includes the Technology Service Providers (TSPs), Sellers and other ONDC Network Participants who may not have any direct contractual relationship with ONDC but are engaged by the Network Participants in relation to activities carried over the ONDC Network.

#### 4. Life cycle of a transaction over ONDC Network

4.1 The stages in the life-cycle of a transaction are:

- **Search and discovery** – This stage will involve the following steps:
  - A Buyer will initiate search for a product or service through the Buyer side Application;
  - Buyer side Application will relay this request to the Gateway;
  - The Gateway will check with the ONDC Registry to identify the relevant Seller side Applications to which Onrecord Sellers are registered that have the requested products or services available in the specified location. Upon identification, the search request will be broadcast to the relevant Seller side Applications;
  - Seller side Application shall relay the information to the Onrecord Sellers listed on their platform to confirm the offering of the product or service requested, along with the terms and conditions of the offering.
  - Upon Onrecord Seller's confirmation, Seller side Applications will relay the offer to the Buyer side Application.
  - The Buyer side Application will display the offers to the Buyers.
- **Placing an order** – This stage will involve the following steps:
  - Once Buyer is satisfied with the offering, the Buyer will confirm the purchase of the product and the Buyer side Application will place the order with the Onrecord Seller through the Seller side Application. Upon Onrecord Seller's confirmation, the Seller Side Application will confirm the order on behalf of the Onrecord Seller.
  - Every transaction undertaken on the ONDC network is governed by a transaction level contract between the Buyer and the Onrecord Seller. The transaction-level contract is a digital artefact that governs the terms of a given, individual transaction on the ONDC Network, and it is executed through the ONDC Protocol.
- **Payment and settlement** - In this stage, the Buyer completes payment for their purchase, and the entities involved in the transaction get paid their dues. Under the payment and settlement construct on the ONDC network, the collector Network Participant may be a Buyer or Seller side Application. In case of cash on delivery, the Logistics Service Provider ("LSP") will be the Collector. The Network Participants will enter into separate collection and settlement terms with each other.

- **Fulfilment** - This stage will involve the following steps:
  - Onrecord Sellers would need to keep the order ready for delivery;
  - Logistics arrangement can be between Seller side application and Logistics Service Provider (“LSP”) and/or Buyers and LSP. Additionally logistics arrangement can be provided by Onrecord Sellers.
- **Returns/ refunds/ cancellations** – Returns/cancellations may be initiated by Buyers. Refund in case of returns, cancellations, damaged items will be processed either by the Buyer side or the Seller side Application depending on which Network Participant collected the buyer price. If a Buyer initiates a refund for Cash On Delivery (“COD”) Order after acceptance of delivery, the entity procuring the services of the LSP and receiving the buyer price from the LSP will initiate the refund to the Buyer.
- **Scoring and Badging** - On completion of each transaction, the Buyer will be required to rate and/or review the transaction based on their experience. The information related to such scoring shall be shared by Network Participants with ONDC.

## 5. What is fraud?

### Principles of fraud/misconduct as per various statutes

- 5.1 Fraud is any activity that relies on deception to achieve a gain. Fraud becomes a crime when it is a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.
- 5.2 Fraud in relation to affairs of a company or anybody corporate 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<sup>1</sup>.
- 5.3 Fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:
- the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
  - the active concealment of a fact by one having knowledge or belief of the fact;
  - a promise made without any intention of performing it;
  - any other act fitted to deceive;
  - any such act or omission as the law specially declares to be fraudulent<sup>2</sup>.

---

<sup>1</sup> Refer to Section 447 of the Companies Act 2013.

<sup>2</sup> Refer to Section 17 of the Indian Contract Act 1872.

- 5.4 Fraud includes any act, expression, omission or concealment committed whether in a deceitful manner or not by a person or by any other person with his connivance or by his agent while dealing in securities in order to induce another person or his agent to deal in securities, whether or not there is any wrongful gain or avoidance of any loss, and shall also include:
- a knowing misrepresentation of the truth or concealment of material fact in order that another person may act to his detriment;
  - a suggestion as to a fact which is not true by one who does not believe it to be true;
  - an active concealment of a fact by a person having knowledge or belief of the fact;
  - a promise made without any intention of performing it;
  - a representation made in a reckless and careless manner whether it be true or false;
  - any such act or omission as any other law specifically declares to be fraudulent,
  - deceptive behavior by a person depriving another of informed consent or full participation,
  - a false statement made without reasonable ground for believing it to be true.
  - the act of an issuer of securities giving out misinformation that affects the market price of the security, resulting in investors being effectively misled even though they did not rely on the statement itself or anything derived from it other than the market price<sup>3</sup>.

### **Definition of Fraud in the context of ONDC**

- 5.5 While definition of fraud has been defined under various statutes, following illustrative key parameters and criterion may be considered to decide whether an act is a fraud in the context of ONDC network:
- **Intent to defraud** –Network Participant or an End User acts knowingly and has a deliberate objective or purpose to cheat or deceive another Network Participant, End Users and/or ONDC.
  - **Misrepresentation** – Incorrect representation of facts by Network Participants or End Users.
  - **Intent to gain undue advantage** - Network Participant or an End Users conducts an act with an objective or a purpose to obtain an advantage that would not have been obtained in normal course of business.
  - **Abuse of position** - Network Participant or an End Users abuses his position dishonestly to obtain a gain or cause loss to another Network Participant, End Users or ONDC.
  - **Personal profiteering** – Network Participant or End Users takes advantage of a situation to make money that was not due to them.

---

<sup>3</sup> As per Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003.

- **Undisclosed conflict of interest** – Undisclosed affiliation/relationship between Network Participants.

5.6 **Potential red flag transactions:** In addition to the above-mentioned parameters and criteria, review of transactional data by the Network Participants may also indicate potential red flag transactions. Such transactional data may be looked at by the Network Participants to identify if an Onrecord Seller is a bad actor. Multiple or repeated transactions (beyond reasonable threshold)<sup>4</sup> wherein requisite transaction fulfilment criterion are not met may be considered as red flag transactions. Following are illustrative operational parameters not met by End Users that may be considered to identify such bad actors:

- Negative customer reviews
- Unsuccessful delivery against orders accepted by the on-record seller
- Delayed delivery of orders
- Delayed/incorrect/no refunds to Buyers

Network Participants may define a reasonable threshold depending on operational parameters beyond which identified red flags in the transactions can be classified as potential fraudulent act defined under section 5.5 by End Users.

### **Illustrative Fraud scenarios on the ONDC network**

5.7 While conducting business on the ONDC network, NPs may face situations that may be indicative of potential fraud. These could relate to onboarding of Sellers and/or Buyers by NPs as well as transactions that may be undertaken through the Seller side or the Buyer side Application. Some illustrative examples of such fraudulent instances could be as follows:

- On record Sellers/ Seller side Applications with history of wrongdoings, corrupt past behaviors uses different identity (i.e., using a new KYC/GST identification) registers afresh with the same/different Seller side Applications or ONDC without getting noticed.
- Onrecord seller/Inventory seller falsely declares incorrect product, product category, SKU, brand etc when compared to its actual catalogue. As a result, incorrect search results displayed to Buyers using ONDC network leading to possible incorrect order placed on the ONDC network.
- Seller side Application in lieu of excess commission/fees from certain Onrecord Sellers does not broadcast the other Onrecord Sellers offering similar products/services, as a response to search made by Buyers on the ONDC network.
- Sellers Onrecord and/or Inventory Seller misrepresents the brand and quality, description of products/ services at ordering stage or uses ingenuine, counterfeit, look alike, non-branded products during fulfillment of the orders.

---

<sup>4</sup> NP's may define a reasonable threshold depending on nature of operational parameters not repeated met by End Users.

- Existing E-commerce entity registers on the ONDC network as a Buyer side Application, uses discriminatory filtering methods to show its affiliated Onrecord Sellers as top search result to the Buyers registered on its Buyer side Application.
- Buyer side Application colludes with certain set of Buyers with past identified fraudulent/corrupt behaviors and continues to broadcast searches of such Buyers to Gateway over the ONDC network.
- Gateway get registered on the ONDC network without disclosing its affiliates who are registered on the ONDC network as Buyer side Application and Seller side Applications.

For the exhaustive list of fraud scenarios, refer “**Fraud Risk Universe tab**” in Fraud Risk Universe and Monitoring mechanism document.



## 6. Operationalization of fraud prevention controls

6.1 The Network Participants transacting over the network may come across transactions that may potentially be fraudulent in nature, related to onboarding of Buyers and/or Sellers, order generation and fulfilment, and post fulfilment of the orders as well. In order to mitigate such fraud risk scenarios and safeguard the interests of both, ONDC network and the Network Participants, following methodologies may be undertaken for fraud risk management:

### **Due diligence of Onrecord Sellers**

6.2 It is recommended that Network Participant may perform due diligence procedures on the Onrecord Sellers, as the case may be at the time of onboarding. The due diligence procedures shall include an assessment of the Onrecord seller, as the case may be on various risk profiles<sup>5</sup> such as:

- KYC assessment – Verification of the genuineness of the KYC documents provided
- Financial risk – assessment on the business sustainability indicators, involvement in financial crimes
- Political risk – Association with political parties/politicians
- Regulatory risk – Regulatory non compliances
- Legal risk – Assessment of civil and/or criminal law suits against the on-record seller
- Assessment of the business existence: Verification of the scale and size of the setup

6.3 Categories may be defined for each of the Onrecord Seller depending on the scale of operations and a combination of one or more of the above risk profiles may be assessed by the Network Participants, depending on the category of the Onrecord Seller.

For details, refer “**Network Participant due diligence tab**” in Fraud Risk Universe and Monitoring mechanism document.

### **Audits and monitoring**

6.4 A risk-based monitoring methodology for evaluation of fraud risk may be undertaken by the Network Participants. The methodology shall focus on proactive audit monitoring procedures and ongoing monitoring procedures based on certain triggers<sup>6</sup>. It shall also focus on improvement of the prevention and detection techniques. These procedures and techniques shall include:

---

<sup>5</sup> Categorization of End Users as large and medium/small may be based on pre-determined thresholds of i) turnover ii) scale of operations iii) Nature of services and products (iv) Listed public limited company or any other parameter deemed fit by NPs.

<sup>6</sup> Trigger can include but not be limited to the following a) Certain set of NP's/Onrecord Sellers continuously defaulting on operational parameters like NP/Onrecord seller ratings, customer complaints on IGM, order fulfillment etc. b) Certain set of NP's are audited post defined number of years said NP's have been on ONDC network c) Outliers/exceptions observed on certain NPs/ Onrecord Sellers from the continuous data monitoring

- 6.5 **Transaction Audit:** Network Participants may perform review of the transactions undertaken by the Onrecord Sellers and/or Buyers to identify any trends/patterns which may be indicative of potential fraudulent/red flag transactions. Review of the transactions will help the Network Participants identify such bad actors and prevention/remediation measures such as real time monitoring etc. may be undertaken to prevent such transactions.
- 6.6 **Field visit and Site Audit:** Field visit may be undertaken by the Network Participants to ensure that the Onrecord Sellers are fulfilling the orders adequately. Field visit may be undertaken to monitor multiple performance criterion such as timely delivery of orders, quality of the products delivered, return and refund management process of the Onrecord Sellers. Based on the assessment of the Onrecord Sellers through field visit activity, the Network Participant may undertake remediation measures such as real time monitoring, providing feedback to the Onrecord Sellers etc.
- 6.7 **An Information Technology audit** is conducted for examination and evaluation of Network Participant's information technology infrastructure, applications, data use and management, policies, procedures and operational processes against recognized standards or established policies.
- 6.8 **Sentiment analysis/Social audits** from social networking properties around customer dissatisfaction, fraud/ misconduct, and any other negative brand publicity.

For details, refer “**Network Participant Audit Monitoring tab**” in Fraud Risk Universe and Monitoring mechanism document

### **Real time continuous monitoring**

- 6.9 Based on the nature of outcome noted from audits and monitoring, Network Participant may categorize the on-record Sellers into categories for real time monitoring. Based on the category of the on-record Sellers, various real time monitoring measures may be undertaken by the Network Participant such as restriction on the transactions undertaken by the identified on-record Sellers for a particular time frame etc.

For details, refer “**Continuous Monitoring tab**” in Fraud Risk Universe and Monitoring mechanism document

## **7. Recommended action points in context of Fraud Risk Management**

Fraud risk management is to be followed over a period of time and it takes time and effort to develop and implement controls for fraud prevention and detection. The Network Participants may undertake following action points to implement an effective fraud prevention framework for transacting on ONDC network:

- Network Participants may enable operationalization of fraud prevention controls for timely prevention and detection of fraudulent activities/red flag transactions. Fraud Risk monitoring mechanism are detailed under paragraph 6.1 to 6.9.
- It is recommended that Network Participants inform ONDC about fraudulent activity/incident, if any that may come to their attention pertaining to the transactions undertaken on the Network by the End User, including but not limited to the following:
  - Procedures undertaken by the Network Participant to investigate the fraudulent activity/incident
  - Modus operandi adopted by the on-record Sellers/Buyers for conducting the fraudulent activity/incident
  - Control gaps in the infrastructure of the Network Participant that led to the occurrence of the fraudulent activity/incident
  - Remediation measures undertaken by the Network Participant to mitigate the identified control gaps.
- Pursuant to paragraph 6.9, NP's are recommended to keep a record of the outcome from the continuous monitoring procedures undertaken which can be requested by ONDC, as and when required.
- Pursuant to clause 2.1.10 of Chapter 2 of Business rules v.1.0, ONDC may request the Network Participants for submission of transactions data in regard with fraud risk management.
- The Network Participants may analyze and review the data pertaining to Issue and Grievance Management system and maintain details of the complaints which indicate potential fraud by the End Users. Aforesaid information can be requested by ONDC, as and when required.

## Glossary

#	Acronym/Term	Full form along with definitions
1	ONDC	Open Network for Digital Commerce
2	NP	Network Participants shall include Seller side Applications, Buyer side Applications and Gateways.
3	End Users	Shall include Onrecord Sellers and Buyers registered on Seller side Application and Buyer side Applications respectively.
4	LSP	Logistics Service Provider
5	COD	Cash On Delivery
6	MSN	Marketplace Seller Node
7	ISN	Inventory Seller Node
8	KYC	Know Your Customer
9	SKU	Stock Keeping Unit
10	Onrecord Sellers	Sellers registered with the Seller side Applications
11	Buyers	Buyers registered on the Buyer side Applications