Ecommerce Fraud Detection Policy
Version 1.1

POLICYBAZAAR INSURANCE BROKERS PRIVATE LIMITED

Ecommerce Fraud Detection Policy
Effective from: 14th June 2021
(Approved by the Board at its meeting held on 14th June 2021)
Version 1.1
Ecommerce Fraud Detection Policy
Version 1.1

Document Control

<table>
<thead>
<tr>
<th>Type Of Information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title</td>
<td>Ecommerce Fraud Detection Policy</td>
</tr>
<tr>
<td>Document Code</td>
<td>POLICYBAZAAR INSURANCE BROKERS PRIVATE LIMITED _ Ecommerce Fraud Detection Policy v1.1</td>
</tr>
<tr>
<td>Date of Release</td>
<td>14th June 2021</td>
</tr>
<tr>
<td>Document Version No.</td>
<td>1.1</td>
</tr>
<tr>
<td>Document Owner</td>
<td>Department Heads</td>
</tr>
<tr>
<td>Document Author(s)</td>
<td>Legal &amp; IT Department</td>
</tr>
<tr>
<td>Document Approver</td>
<td>Board of Directors</td>
</tr>
<tr>
<td>Security Classification</td>
<td>External</td>
</tr>
</tbody>
</table>

Document Revision History

<table>
<thead>
<tr>
<th>Ver. No.</th>
<th>Date</th>
<th>Change Description</th>
<th>Author</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>14th June 2021</td>
<td>Initial Release</td>
<td>Legal &amp; IT Department</td>
<td>Principal Officer</td>
</tr>
<tr>
<td>1.1</td>
<td>9th August 2022</td>
<td>Annual Review</td>
<td>Legal &amp; IT Dept.</td>
<td>Board of Directors</td>
</tr>
</tbody>
</table>
Table of Contents:

1. Introduction.......................................................................................................................... 4
2. Objective and Scope of the Policy ......................................................................................... 4
3. Definition and Categories of potential e-commerce Fraud...................................................... 4
4. Indicative Areas of e-commerce Fraud..................................................................................... 5
5. Fraud Management and Governance Structure........................................................................ 5
6. Reporting Procedure................................................................................................................ 6
7. Implementation, Monitoring and Review .................................................................................... 6
Annexure A .................................................................................................................................. 7
1. Introduction

This E-commerce Anti-Fraud Policy ("Policy") is framed by Policybazaar Insurance Brokers Private Limited ("the Company") as per Insurance Regulatory and Development Authority ("IRDAI") Guidelines on Insurance E-commerce issued vide circular no. IRDA/INT/GDL/ECM/055/03/2017 dated 9th March 2017.

2. Objective and Scope of the Policy

The objective of this Policy is to put in place effective Fraud Monitoring framework and ensuring that management is aware of its responsibilities for the detection and prevention of fraud and for establishing procedures to prevent fraud and/or detect fraud on its occurrence. This Policy shall provide guidance with respect to detection, prevention, mitigation and investigation into fraudulent activities related to E-commerce and Cyber fraud.

The Company has adopted this policy to ensure consistent and effective investigation, reporting and disclosure of fraud occurrences and to provide a clear guidance to the employees and others dealing with the Company, forbidding them from involvement in any fraudulent activity and the action to be taken by them when they suspect any fraudulent activity.

3. Applicability

This document applies to all employees and officers of the Company at whatever level, at every location and whatever the terms of employment, hours of work or length of service, including contractual staff and directors in the employment of the Company, as well as shareholders, service providers, consultants, vendors, contractors and subcontractors, prospective and existing customers and/or other parties with a business relationship with the Company.

4. Definition and Categories of potential e-commerce Fraud

"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;

"Wrongful gain” means the gain by unlawful means of property to which the person gaining is not legally entitled;

"Wrongful loss” means the loss by unlawful means of property to which the person losing is legally entitled.
Categories of Frauds:

1. **Internal Fraud**: Fraud, mis-appropriation, mis-representation against the Company by its Director, Manager and / or any other officer or staff member (by whatever name called).
2. **Third Party Frauds**: Any fraud done by a party other than the persons connected with the Company will come under Third party fraud.
3. **Online Fraud**: This type of fraud could inter-alia involve any fraud committed while buying online policy on the Company’s digital platform.

An illustrative list of frauds (online / offline) is mentioned under Annexure A.

5. **Fraud Management and Governance Structure**

The Company shall constitute a Fraud Management and Governance Team (“FMGT”) which to review, recommend the policies, procedures and control mechanism to identify, detect and report insurance frauds. The FMGT shall also be responsible to review the findings of the investigations done and recommend the appropriate actions there upon. The primary administration of the functions of the FMGT will rest with Principal Officer & Chief Executive Officer to carry out the same in coordination with the various departmental heads and business functions.

FMGT will be constituted with the following members and it will report its findings/recommendations to the Principal Officer & Chief Executive Officer:

- IT SPOC
- Legal & Compliance SPOC
- Business and Operations SPOC

For any interdepartmental support required by the FMGT, it shall have powers to invite SPOCs from other departments on a need basis.

The FMGT shall more specifically be responsible for the following:

i. **Manner of detecting and identifying frauds** i.e. Laying down process and procedures to identify, detect and report frauds.
ii. **Follow-up mechanism** to take appropriate actions against persons who committed frauds
iii. **Cooperation amongst market participants** to identify frauds and trying to mitigate the risk
iv. **Building database** of those committing frauds and sharing with other market participants.
v. **Awareness among employees/policyholders** to counter insurance frauds.
6. Reporting Procedure

If any fraud (instance of actual or suspected fraud) comes to the attention of an employee, staff member or a customer he/she must report the same to grievance@policybazaar.com

Any employee or customer can also make a protected disclosure ("whistleblower") in writing, duly signed by him, to the FMGT Committee as soon as possible but not later than 15 consecutive days after becoming aware of the same.

If initial enquiries by the FMGT Committee indicate that the concern has no basis, or it is not a matter for which investigation be pursued under this Policy, it may be dismissed at this stage and the decision is to be documented. Where initial enquiries indicate that further investigation is necessary, this will be carried through by the FMGT Committee or by any other person as nominated by the Committee for this purpose. The investigation would be conducted in a fair manner, as a neutral fact-finding process and without presumption of guilt. The name of the Whistle Blower would be kept confidential.

A Protected Disclosure may be made anonymously by writing to:

Fraud Management and Governance Team
Policybazaar Insurance Brokers Private Limited
Plot No. 119, Sector-44, Gurugram-122001, Haryana

If a protected disclosure is made anonymously or otherwise, the Protected Disclosure must provide as much detail and be as specific as possible with respect to the fraudulent activity as defined under this policy, including names and dates, in order to facilitate the investigation.

Reporting to Law Enforcement: On a case-to-case basis, where it is reasonably believed that a fraud has been committed, the Company may report the case to appropriate law enforcement authorities.

7. Monitoring and Review

FMGT will review the policy at least annually in line with the Company Business, Products and Process and shall align with the amendment any regulatory guidelines that may be issued from time to time, for effective deterrence, controls, prevention, detection and mitigation of frauds. Any revised version shall be submitted to the Information Security Officer along with the FMGT for its review and further recommendation to the Board of Directors for approval.
ANNEXURE A

A. INDICATIVE LIST OF DIFFERENT TYPES OF FRAUDS

The various type of Frauds that normally is being faced by an online Insurance Intermediary can be classified as below. This list is only a Comprehensive list but not an exhaustive list.

a. Misrepresentation of facts in the Proposal/ Claim form or any other document.
b. Misappropriation of funds.
c. Non-disclosure of material facts.
d. Wrong information pertaining to the claim.
e. Wrong information on the exact cause of loss/damage.
f. Claiming for fictitious damages/loss.
g. Submitting of forged documents by customers.
h. Employee involvement in making fraudulent insurance policies.
i. Employee involvement in Forging details of the customer in the proposal form, policy document, or any other document to defraud the Company.
j. Stealing company assets like laptops, computers, cover notes etc.
k. Manipulation/stealing/sharing of Customer data & information in an unauthorized way.
m. Issuing fraudulent policies in the name of the insurance companies (i.e. business partners of the Company) and misrepresenting on behalf of the Company and siphoning of premium amount.
n. Transactions effected through fake or stolen credit card/bank accounts to carry out a transaction in the web portal of the Company.
o. Confidential data of the Company being comprised due to any cyber-attack/hacking of the Company systems.
p. Any other type of online fraud.
q. Compromise due to phishing and malware

B. INDICATIVE AREAS OF E-COMMERCE FRAUD

a. Illegal hacking.
b. Confidential Company data being compromised due to cyber-attack/ illegal hacking/ access of Company network connection.
c. Bogus online activity generated in an attempt to generate illegitimate revenue.
d. Transactions carried out on Company website using fake/ stolen credit card or bank account details.
e. Compromised mail accounts/ Detection of defacement/intrusion of website.

Please Note: The above list is only illustrative and not exhaustive.