Tata AIG General Insurance Company Limited

Anti-Fraud Policy and Guidelines

Tata AIG General Insurance Company Limited

Anti-Fraud Policy and Guidelines

Version 5: Document History and Version Control	
Name	Anti-Fraud Policy and Guidelines
Review of Policy	On Annual Basis
Document Owner	Enterprise Risk Management

Version Number	Board Approved Date	Revised / Modified By	Reviewed by	Change Incorporated
Version 4	12-June-2020	Satyanandan Atyam	Ethics Committee	Revised with reference to Industry leading practices, in line with Tata Code of Conduct & IRDAI regulations
Version 4	20-Jan-2021	Satyanandan Atyam	Ethics Committee	Annual Review – No change
Version 5	03-Feb-2022	Satyanandan Atyam	Ethics Committee	Annual Review – **replaced IRC with Ethics Committee in section 6.1 (a)**
Version 5	14-Feb-2023	Satyanandan Atyam	Ethics Committee	Annual Review – C**hange incorporated:** 1. Record Retention – Minimum tenure of record retention changed to 12 years from 7 years to align with Data Retention Policy
Version 6	02-Feb-2024	Satyanandan Atyam	Ethics Committee	Annual Review – No change
Version 7	05-Feb-2025	Satyanandan Atyam	Ethics Committee	Annual Review – No change

1 Contents

2 Introduction

2.1 Background

1. Financial fraud poses a serious risk to all segments of the financial sector. Fraud in insurance shakes policyholders' as well as all other stakeholder's confidence and can affect the reputation of insurer and the insurance sector as a whole. It also has the potential to impact economic stability.
2. The Insurance Development and Regulatory Authority of India ('IRDAI'), vide its circular 'IRDA/SDD/MISC/CIR/009/01/2013' dated 21 January 2013, called upon all insurers in India to recognize and assess the implication of fraud as a risk management measure and to put in place an effective and comprehensive policy to deal with fraud.
3. Also, the 'Corporate Governance Guidelines for Insurance Companies' dated 18 May 2016, issued by IRDAI requires insurance companies to formulate a Fraud monitoring policy and frame effective for deterrence, prevention, detection and mitigation of frauds.
4. Further, as laid down in the "Guidelines on Insurance e-commerce" dated March 9, 2017, an insurer is required to have a pro-active fraud detection policy for insurance ecommerce activities, which is to be approved by the Board of Directors. Accordingly, this Policy has been formulated considering the various types of frauds including e-commerce frauds that the Company can be exposed to.
5. Accordingly, Tata AIG General Insurance Company Limited ('Company') has formulated/revised its Anti-Fraud Policy and Guidelines ('Policy') with an objective of conducting business in an environment of fairness and integrity and will strive to eliminate fraud from all operations. The Company adopts a Zero-Tolerance approach to fraud and does not accept any dishonest or fraudulent act committed by internal and external stakeholders.
6. The Anti-Fraud Policy including, any amendment/modifications to the same, shall be reviewed and approved by the Board, through RMC as deemed necessary, but at a minimum on an annual basis.

2.2 Scope

Scope of the Policy includes:

a. Providing an understanding of 'Fraud' and its implications and effects on the Company and ensuring that the management is aware of its responsibilities for the detection and prevention of fraud.

b. Providing a clear guidance on how detection, prevention and investigations into fraudulent activities will be conducted and ensuring protection of those who report frauds in line with the 'protected disclosure' clause (as per the 'Whistle blower policy').

c. Ensuring consistent and effective investigation, reporting and disclosure of fraud occurrences. Providing assurance that the potentially fraudulent activities will be duly investigated and dealt with appropriately. Setting the tone that fraud is not acceptable and shall not be tolerated.

d. Ensuring processes to prevent, detect and manage frauds as well as ensuring that the preventive measures are continuously enhanced, strengthened and implemented in a speedy manner.

2.3 Applicability

a. The Policy shall be applicable to all employees and officers of the Company, and contractual staff, trainees, retainers, agents, other insurance intermediaries, service providers, consultants, vendors, policy holders, contractors and sub-contractors, associated with the Company.

3 Definitions

3.1 Terminologies used in the policy

a. **"Company"** means "Tata AIG General Insurance Company Limited"

b. **"Employee"** means any person employed by the Company (probationer, confirmed or outsourced), including former employee and Directors of the Company (whether working in India or abroad).

c. **"Ethics Committee" (EC)**. The Ethic committee working will be guided by a pre-defined charter, which specifies the committee's mission, objective, composition, authority, frequency of meetings, amongst others.

d. **"Fraud Control Unit (FCU)"** means the team entrusted with the responsibility to perform and/or oversee investigations of the reported frauds.

e. **"Investigating Team"** refers to those persons authorized, appointed, consulted or approached by the Head FCU /Ethics Committee and may include FCU OR Independent Investigation Agency or other experts like forensic/ computer forensic.

f. **"Policy or This Policy**" refers to the 'Anti-Fraud Policy and Guidelines'

g. **"Risk Management Committee"** carries the meaning as described in 'Corporate Governance Guidelines for Insurance Companies' dated 18 May 2016.

h. **"Claims -Special Investigating Unit (SIU)"** means the unit formed to handle, fraudulent activities specifically for the Insurance claims frauds.

i. **"Suspect individual"** means the individual or representative of an entity potentially involved in perpetrating the fraud.

3.2 What constitutes 'Fraud'

a. IRDAI defines 'Fraud' in Insurance sector to mean an act or omission intended to gain dishonest or unlawful advantage by a party committing the fraud or for other related parties which may, for example, be achieved by means of:

- Misappropriating assets;
- Deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of the insurer's status;
- Abusing responsibility, a position of trust or a fiduciary relationship;

b. Fraud may also include any other non-compliances to the Companies code of conduct; online frauds; cyber-attacks; 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.

c. The company may also be exposed to cyber/digital or online frauds perpetrated by third parties and/or employees.

3.3 Broad categories of fraud

a. The frauds may be perpetrated against the Company by policy holder; intermediaries (insurance agents, brokers, distributers, vendors, consultants, contractors, third party administrators etc.), or internally by Directors of the Company irrespective of their employment or by employees including full time employees, part time employees, employees on contract, outsourced employees and any unrelated party. *An illustrative list types of fraud is enumerated in Annexure 1*

b. The frauds would also include cyber threats such as illegal hacking, cyber-attack, denial of services, credit card theft, data leakage incidents amongst other. *An illustrative list types of fraud is enumerated in Annexure 2*

4 Fraud Risk Management Framework

Functional departments are the first line of defense and hence responsible for the detection and prevention of fraud, misappropriation and other inappropriate conduct. It is the primarily responsibility of every function to implement and manage processes to ensure that sufficient controls to detect and prevent frauds are in place. Indeed, each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of any irregularity.

This framework aims to ensure that the Company is adequately equipped to protect its brand, its reputation and its assets from loss or damage resulting from suspected or confirmed incidents of frauds / misconducts. The framework comprises:

- Reporting and investigation of potential frauds
- Fraud prevention controls, and
- Creating awareness.

4.1 Reporting and investigation of potential frauds

4.1.1 Fraud reporting channels

Any employee/third party who suspects dishonest or fraudulent activity shall notify to the Ethics Committee immediately, at the email ID conduct@tataaig.com. *Refer Annexure 3 for prescribed format of reporting.*

a. The Ethics Committee will be constituted as per the charter of the committee.

b. All the frauds detected by any department and/or detected by any person with knowledge of confirmed, attempted, or suspected fraud or any person who is personally being placed in a position by another person to participate in fraudulent activity shall be reported to and by the functional head within 48 hours from the detection of any confirmed, attempted or suspected fraud.

c. Any fraud known to one or more Company's employees being not reported will be considered very serious and disciplinary actions will be initiated against the person withholding the information.

4.1.2 Investigation responsibilities

a. FCU will be responsible to formulate and maintain the necessary procedures for investigation, and that they comply with the local laws and regulations. These procedures must be reviewed by the CRO & Ethics committee on a regular basis.

b. Based on the sensitivities of the case (to be decided by the Ethics Committee), Ethics Committee may also decide to appoint an independent investigation agency to investigate a case (end to end) and choose not to involve the FCU.

c. FCU may seek assistance from an independent investigation agency or any other experts including forensic/ computer forensic ('investigating team'), if required based on merit of each case. The appointment of such party/s shall be approved by the Ethics Committee.

d. No employee/third party shall attempt to personally conduct investigations or interviews/ interrogations related to any fraudulent/potentially fraudulent act, unless directed by the Ethics Committee.

e. The FCU will maintain a centralized internal fraud database where all internal fraud data losses and recoveries will be logged. Upon discovery or reporting of an internal fraud case, the FCU will open a case file and log the case in the centralized internal fraud database and assigns a unique case number to the case, to help track the case lifecycle.

f. FCU will keep Internal Audit informed about all cases referred to FCU for investigation and take their inputs during investigations as required

g. In case, the allegation was against (or could be involved in anyway) any member(s) of Board / Ethics committee, the Ethics committee will intimate the MD & CEO and Chairman of RMC-within 48 Hours of receipt of the complaint. In such cases, investigation shall be conducted under guidance and direction of MD / chairperson RMC and the report shall be submitted to RMC who would decide the further course of action/ disciplinary action.

h. FCU / Investigation Team (as the case may be) shall present its finding to the Ethics Committee. The Ethics Committee will examine the investigation findings and issue its recommendation, within seven days of receipt of investigation report from FCU, to HR and to respective department head for implementation.

i. In case, the allegation was against the respective department head, report may be issued to suspect individual's reporting supervisor, or as found necessary by the Ethics Committee, for implementation of recommendations.

j. Head FCU under supervision of the Ethics committee, of the company shall be the nodal officer responsible for coordinating with law enforcement agencies to report fraud cases on a timely and expeditious basis, and to deal with the follow-up processes.

4.1.3 Investigation

a. Utmost care must be taken in the investigation of potential improprieties or irregularities to avoid mistaken accusations or alerting suspect individuals that an investigation is under way.

- **How it happened**: The fraud investigation shall consist of gathering sufficient information about specific details and performing procedures that may be necessary to determine whether fraud occurred, the loss or exposures associated with the fraud, who was involved in it and the fraud scheme.
- **Free access**: The members of the FCU will have free and unrestricted access (as required for respective case) to all Company records and premises, whether owned or rented, and the authority to examine, copy and/or seize/taken into custody or any portion of the contents of files, desks, cabinets and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.
- **Disclosure to the suspect individual:** The individual or representative of an entity potentially involved in perpetrating the fraud (suspect individual) may be informed of the allegations as soon as reasonably practicable. This may not be done until the initial stages of the investigation have taken place. The Ethics Committee may decide to not inform the suspect individual about the allegations, in case allegations were not proved against him/her. This is to avoid hampering the motivation of any employee.
- **Investigation support -** All members associated to the investigation (including the whistle blower, suspect individual/s, other stakeholders (such as process owners, approvers, witnesses) will support the investigation team in every possible way. They will be present for the interviews / discussions when called for; they will provide complete and accurate information to the best of their knowledge and ability. This will include providing responses to follow-up questions raised by investigating team during and post conclusion of the investigation.

  The FCU is required to adhere to pre-determined standard operating procedures, which prescribes the method, timelines and mode of interacting with whistleblower, suspects and/or witnesses and the disciplinary action process.
- **Legal compliance:** Appropriate legal consultation (internal and external counsel) may be sought by the investigating team to ensure compliance with all applicable legal requirements including ensuring that the findings and evidences are admissible in court of law.
- **Documentation**: The investigation team shall take into custody all relevant records, documents and other evidence to protect them from being tampered with, destroyed or removed by the suspect individuals or by any other party under his/her influence. The full records of the investigation, including interview notes, shall be kept secure. Head FCU shall maintain & archive records of all documents / data pertaining to all cases reported under this policy.

4.1.4 Corrective actions

a. Ethics Committee may decide (by majority vote), any or more than one of the following actions, or as may deem necessary based on the facts of the respective case:

- Employee dismissal / suspension without pay;
- Termination of a contract;
- Business process/internal control remediation;
- Demotion and/or warning;
- Register First Information Report/ police complaints against the fraudulent individual;
- Recover loss caused by fraudulent activity from the fraudulent employee/vendor;
- Initiate legal proceedings against the fraudulent individual/group of individuals;
- May choose to send the suspect individual on leave till conclusion of investigation. Ethics Committee may also block the system access rights of the suspect individual if found necessary during the investigation;
- May choose to suspect all business operations with third party/s, if suspected to be involved in any fraud on the Company.

b. Ethics Committee shall advise the action plan to the Department Head/ Function head/HR and they will be responsible for implementing the same.

c. The FCU will follow up with Department Head/ Function Head / HR/Legal departments with a view to ensure timely execution of the decisions taken by Ethics committee and give a status / completion report.

d. Fraud shall be reported to the relevant law enforcement authorities, based on the investigation findings and merit.

e. The potential / actual frauds pertaining to the Insurance claims of the Company will continue to be managed by the 'Claims Function, along with Claims-SIU (Special Investigation Unit). However, if any guideline of claims policy is in contradiction of this policy then this policy will have overriding effect on claims policy.

4.2 Fraud Prevention Controls

Fraud generally perpetrate due to failed/inadequate/poorly implemented controls. Therefore, periodic review of controls to assess the gaps and implementing effective controls is an imperative part of fraud monitoring framework. Following are some examples of proactive fraud prevention strategy:

a. **Tone at the top** - The Board of Directors, managers and officers set the 'tone at the top' for by behaving ethically and openly communicating expectations for ethical behavior to employees.

b. **Risk assessment** - All functional heads are responsible for day to day management of activities and in charge of maintaining, implementing and improving their systems and controls to minimize the possibility of fraud. Functional heads shall

have a process in place for continuous quality check of their functions, and to conduct fraud risk vulnerability assessment of their processes. The gaps identified through these assessments along with the remediation plan should be shared with the FCU. Ethics Committee shall ensure implementation of the remediation plan.

The data breaches due to cyber-attacks and data leakage incidents from DLP (Data Leakage Prevention) solution will be presented by the Chief Information Security officer to the Ethics committee based upon a pre-determined standard operating procedure.

c. **Plug process gaps**: The functional heads shall also steer Company's efforts to address the control weaknesses/ procedural deficiencies that get highlighted during investigation, to prevent their recurrence. The gaps may be highlighted jointly by the FCU and the internal audit team.

d. It is the responsibility of the Chief Information Security officer to ensure appropriate controls are in place with respect to cyber security.

e. **Independent review of control effectiveness -** The FCU (under the guidance of the Ethics Committee) shall be responsible for defining the procedures to identify, detect, investigate and report frauds. The FCU will use analytical tools to identify potential fraud areas and then follow it with sampling methodology to identify patterns, if any. Committee shall put in place corrective and preventive measures basis the review performed. Committee shall also spread awareness regarding fraud prevention across the organization to develop a culture of zero tolerance.

Independent audits shall be carried out if required to provide an assessment of design and control effectiveness.

Background verification - The Human Resources department shall ensure that pre-employment verification is done before appointing persons for every job. Similarly, precautionary steps will be taken by the respective functions to ascertain the antecedents of insurance agent/corporate agent/intermediary/TPAs before appointment/ entering into agreements with them.

4.3 Trainings and Awareness

a. The Company recognizes that proper awareness is the main pillar of fraud prevention effort. The Ethic Committee shall also evaluate the need of any Training & Awareness Program to sensitize its employees/agents/vendors on the dangers posed by engaging in such acts, not only to the Company but also to the employee/agent/ vendor.

b. Regular and periodic training (including new-hire orientation and refresher training) shall be provided to all personnel, upon joining the organization and throughout their association with the Company, in order to clearly communicate expectations for ethical behavior to staff members; Such training shall also include an element of 'fraud awareness' and communication of responsibilities. As far as possible, training should be specific to the employee's level within the Company, geographic location and assigned responsibilities. Examples of the types of fraud that could occur, and the potential perpetrators shall be provided in the course of the training.

c. The Company shall aim at continuously educating its employees, customers and the general public on fraud prevention and enlist support and participation in fraud prevention.

d. The Company shall do the fraud mitigation communication within the organization at periodic intervals and/or adhoc basis, as may be required and shall also ensure the information flow amongst the various operating departments.

e. This Anti-Fraud Policy document shall be published on the intranet site of the Company.

f. All employees including senior management employees are required to sign (either electronically or manually) a confirmation statement at least annually, acknowledging that they have read, understood and complied the Anti – Fraud Policy Statement of the Company.

5 Confidentiality and Protection

5.1 Confidentiality

a. The FCU/investigating team shall treat all information received confidentiality. The detailed investigation results shall not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct.

The FCU members are required to sign a confidentiality agreement as per pre-defined format, specifically requiring them to abide the requirements of this policy.

b. The investigations shall always be kept at confidential and private as possible to ensure the least amount of disruption to the Company and maintain the process integrity. Confidential information will be shared only on a 'need-to-know' basis.

5.2 Exchange of information pertaining to investigation

a. The Company's belief is that, just as good work needs to be encouraged through awards/ promotions etc., financial impropriety needs to be strongly discouraged. The Company may blacklist vendors/agents/TPAs/intermediaries/agents of intermediaries based on the outcomes of the investigations and at its discretion, publish names, designations, photographs of employees/agents/vendors found involved in such acts in its internal and/or external communication. The backlisting procedures should be in line with internal compliance and regulatory requirement.

b. The CHRO/Head FCU and his team as directed by Ethics Committee shall decide on the need of the communication to all its employees/agents/vendors the action initiated so as to deter others from engaging in similar activities. The Company also believes in exchange of necessary information on frauds, amongst all insurers through the General Insurance Council and/or any other regulatory or otherwise body/organization/mechanism.

c. The Company shall fully support in establishing any industry wide platform set up for the purpose of sharing of company level data/information/ best practices etc.

d. The departmental/ Function head should ensure that fraud awareness should be part of all the functional training conducted by the department for their employees.

5.3 Protection

a. No unfair treatment will be reserved to the person who has reported in good faith a potential incident of fraud. The Company condemns any kind of discrimination, retaliation, harassment, victimization or any other unfair employment practices being adopted against the person who has reported in the fraud.

b. The identity of the person who has reported the potential fraud shall be kept confidential to the extent possible and permitted under the law. However, any abuse of this protection (such as, any false or bogus allegations made by a person knowing them to be false or bogus or with a mala fide intention) will warrant disciplinary action.

c. If any employee or an officer reports a potential fraud for personal gain or to disrupt the working environment or by making the disclosure , would be committing a criminal offence such as blackmail, he/she would not get any protection and his/her behaviour would also constitute a disciplinary offence.

6 Reporting

6.1 Reporting of investigation outcomes

a. The Frauds reported and the investigation outcomes should be submitted by the FCU on a monthly basis to the Ethics committee. On a quarterly basis the FCU head will present the frauds reported, outcomes and key learnings to the Ethics Committee .

b. Internal audit will be kept informed on the investigated cases by FCU from the beginning & constant learnings will be shared by Internal Audit and the FCU team

c. The CRO will present the Frauds reported, key investigation outcomes and learnings to the Audit Committee and Risk Management Committee. The RMC will represent the material outcomes as deemed necessary to the Board of Directors.

6.2 Regulatory reporting

a. The statistics on various fraudulent cases investigated/highlighted and action taken thereon shall be filed with IRDAI in forms FMR 1 and FMR 2 providing details of outstanding fraud cases and closed fraud cases

b. The reporting shall be done, to IRDAI as per guidelines applicable at the time of reporting. Head FCU shall ensure compliance of the necessary regulatory reporting from time to time.

6.3 Communicating with authorities

a. In case complaint or First Information Reports (‘FIR’) is decided by the Ethics Committee in to be filed with any Authority/ Law Enforcement Agencies it shall be done by Department Head/ or any Local Representative of Company in consultation with the Corporate Legal Department. The FIR will be drafted by FCU and will be duly vetted by Corporate Legal Department.

7 Record Retention

a. All Protected Disclosures in writing or documented along with the results of inquiries relating thereto & the MOM of the Internal Committee shall be retained by the Company for a minimum period of twelve years and for a duration over and above twelve years as deemed necessary by the Chief compliance officer and/or legal counsel for specific investigations.

8 Amendment

a. The Company reserves its right to amend or modify this Policy in whole or in part, at any time without assigning any reason whatsoever. However, no such amendment or modification will be binding on the Employees and Directors unless the same is notified to the Employees and Directors in writing.

b. The policy will be reviewed annually by the Ethics committee (EC) to evaluate if any amended and/or modifications are required to the same. The policy will be presented annually for approval to the Board through RMC.

9 Communication of Policy

a. The Company is required to notify and communicate existence and contents of the Policy to the Employees of the Company. The new Employees shall be notified about this Policy by the Human Resource Department. This Policy shall also be uploaded onto the Company's website.

~~b.~~ The Company shall inform both potential and existing clients about their anti-fraud policies. The Company shall appropriately highlight the consequences of submitting a false statement and/or incomplete statement, for the benefit of the policyholders, claimants and beneficiaries.

10 Annexures

10.1 Annexure 1: Illustrative List of Insurance Frauds

Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

Internal Fraud

a. misappropriating funds or impropriety in the handling or reporting of money or financial transactions

b. fraudulent financial reporting

c. stealing cheques

d. overriding decline decisions so as to open accounts for family and friends

e. inflating expenses claims/over billing

f. paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers

g. permitting special prices or privileges to customers, or granting business to favored suppliers, for kickbacks/favors

h. forgery or alteration of any document including but not limited to the Company's insurance policies or insured parties

i. forgery or alteration of checks, bank drafts, or any other financial documents

j. removing money from customer accounts

k. Impropriety in the handling or reporting of money or financial transactions with the intention to deprive.

l. Misappropriation of funds, securities, supplies, or other assets.

m. Profiteering as a result of insider knowledge of company activities.

n. Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company

o. disclosing confidential and proprietary information to outside parties

p. Selling insurer's assets at below their true value in return for payment.

Policyholder Fraud and Claims Fraud

a. Claims fraud - death, critical illness, waiver, Private Medical Insurance or Permanent Health Insurance claim is fraudulently made against the policy. For example, death claims when the event has not happened, fraudulent non-disclosure / misrepresentation. Staging the occurrence of incidents

b. Medical claims fraud

c. Underwriting fraud - where a policyholder or applicant either deliberately misrepresents or deliberately fails to disclose material facts at policy inception (that would materially impact either the terms & conditions applied to a policy of insurance, or the issue/renewal decision itself) for financial gain

d. Assignment fraud -when an insured or owner takes possession of the issued policy, s/he will transfer ownership, or 'assign' the policy for value to a person or entity with no insurable interest in the continuation of the insured person's life.

e. Trustee fraud - Fraud by trustees or potential beneficiaries of defined benefits pensions schemes. Also includes exaggerated deductible expenses.

Intermediary Fraud

a. Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer.

b. Inflates the premium, passing on the correct amount to the insurer and keeping the difference

c. Non-disclosure or misrepresentation of the risk to reduce premiums

d. Commission fraud - insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

10.2 **Annexure 2:** Illustrative List of Cyber Frauds in the insurance sector

a. **Identity theft** - Identity theft results in a cyber-criminal stealing sensitive data and using it to conduct transactions on ecommerce sites. A new form of identity theft is called pharming which sends customers to fraudulent websites. Since

most e-commerce platforms store customer payment information in their databases, it is rather easy to take over control of the account.

b. **Clean fraud** - A cyber-criminal perpetrating clean fraud uses a stolen credit card in such a way that they are able to avoid alerting the fraud detectors. Often this is because the criminal has stolen enough information about the credit card holder that they can easily pass the transaction off as legitimate.

c. **Triangulation fraud** - As the name suggests, this type of fraud requires three key "pillars" to execute properly. First, criminals will create a fake online storefront, where they claim to sell high-target items at low prices. Secondly, the stolen credit card information and personal information collected during this process will be used to order items online and have them shipped to the original card owner. The criminals then use the information to make additional purchases. Since these transactions occur shortly after a legitimate purchase, the fraud will usually remain undetected for weeks, if not months.

d. **Merchant fraud** - goods are offered at cheap prices but are never shipped. The payments are, however, not returned. It is not specific to any particular payment method, but this is, of course, where no-chargeback payment methods (most of the push payment types) come into their own.

e. **Advanced fee and wire transfer scams** - This is the classic "Nigerian Prince" scam. The cyber-criminal asks for money upfront, in return for a lot more money later. While the Nigerian Prince scam is formulated to specifically target individuals, scammers have come up with a practice that targets businesses, specifically ones that provide services. The general formula is that the scammer reaches out to the business via email as a prospective client. They say they want an impressive amount of work from the business, but first, they're working with a third-party company who they need to pay and, for some reason, can't. These reasons may even sound legitimate. They'll ask you to send the third-party business some money, which they assure you will be paid back and far more.

f. **Card testing fraud** – Card testing fraud is the practice of creating and testing the validity of a card number, in order to use it on another website to commit fraud. Fraudster target websites which give a different response for each type of decline: for example, when a card is decline due to an incorrect expiration date, a different response is given, so they know they just need to find the expiration date.

g. **Eavesdropping** – This way an attacker gets access to data paths in the network to "listen in" or interpret (read) the network traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. An attacker may also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

h. **Data Modification** - An attacker modifying the data in the packet without the knowledge of the sender or receiver.

i. **Sniffer Attack** - A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer gets full view of the data inside the packet.

j. **Application-Layer Attack** - An application-layer attack targets application server by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls.

k. **Phishing** - In this case an email asks for user ID, passwords, credit card details and other personal information. The sender seems to be a credit institution that needs a confirmation of some information due to a change in the system. Phishing allows criminals to get access to bank or other accounts and it can be used for identity theft

10.3 Annexure 3: **Fraud Incident Report**

Fraud Incident Report.xls