AA Exchange Company (Pvt.) Ltd.

Consumer Protection Policy

Creation Date: 26-06-2024

Version: 01

Validate By: Board of Directors

Written By: Mehran Khan

Contents

I. Introduction

AA Exchange Company (Pvt.) Ltd. has established a comprehensive Customer Protection Policy to facilitate the development of controls that will aid in managing Customer Protection. AA Exchange Company's intends to promote consistent organizational behavior by providing guidelines and assigning responsibility. The Policy conforms full dedication to protect its customers.

AA Exchange Company provides that unfair or deceptive acts or practices in or affecting customers are declared illegitimate. Management shall provide support to and work with the Auditor, other Divisions involved, and law enforcement agencies in the detection, reporting and investigation of activity impacting customer protection, including the prosecution of off Enders.

AA Exchange Company enforces a variety of other customer protection measures that mitigate specifically defined practices. The company's objective, to work in the best interest of their customers and be responsible for upholding financial customer protection and also be responsible and accountable for the actions of their authorized agents.

The Policy guidelines are as enumerated below:

- To ensure that management is aware of its responsibilities for protecting customers in accordance with local regulations and international standards and best practices;
- To provide clear guidance to employees on how to manage customer protection;
- To provide assurance that all customer protection breach will be fully investigated, reported and;
- To provide training on Customer Protection to employee.

II. Role & Responsibilities

Global framework

An efficient management of the Customer Protection is crucial (i) to identify the area of risks, (ii) to prevent from potential violation processed by employees or external parties (iii) and, to maintain a solid setup. To reach this objective, AA Exchange Company (Pvt.) Ltd. must ensure the **coordination and the independency** of the three lines of defense:

- Customers are said to be the "zero line" of defense. Customers are responsible for their own transactions. They are the one who are often the first aware that an issue occurred in their account. AA Exchange Company (Pvt.) Ltd. will put in place a program to increase customer awareness on customer protection. Also the Company will need to implement an efficient customer complaint escalation process:
- Employees (first line of defense): All employees have a duty to protect their customers. Employees are expected to identify processes and procedures that may be vulnerable to customer protection breaches and to draw such instances to the attention of management in their division or escalate directly to the company's designated Compliance Manager.;
- Risk or Compliance Department (second line of defense): Depending on the size of the organization and depending of the risk exposure, this second line of defense role is to manage the risks whether it is the Risk department, the Compliance department or a dedicated department;
- Audit Functions (third lines of defense).

AA Exchange Company (Pvt.) Ltd. must ensure:

- A coordination of the lines of defense to build and maintain a strong compliance setup and to disseminate a compliance culture among all employees;
- An independency of each function in terms of reporting lines to prevent from any conflict of interest.

Three lines of defense: Main Roles

Employees are responsible for:

- Understanding compliance policies and procedures;
- Implementing, maintaining and adapting compliance policies and procedures into each department;
- Performing tasks related to the Customer Protection Program's requirements in each concerned employee's job description;
- Performing Customer Protection Program requirements in terms of employees', customers' and transactions' monitoring;
- Performing initial and refreshers trainings;
- Identifying and escalating operational risk incidents;
- Ensuring the information and documents linked to operational risk incident case are appropriate, accurate and consistent;
- Recording all relevant documents and information for at least 5 years (or more if local regulators require a longer period);

The Compliance/Risk Department oversees:

- Assessing the good understanding of the Customer Protection Program requirements especially regarding the detection and escalations of related incidents;
- Being the single point of contact for advising about Customer Protection Program and being the knowledge center regarding the Customer Protection risk;
- Ensuring that the hotline to manage internal and external complaints is in place and known by all employees and business relationships;
- Ensuring that the hotline is installed, efficient and known by everyone in the organization;
- Setting up processes for the management of Customer Protection Program cases;
- Producing procedures and policies, communicating and enforcing it throughout the organization;
- Ensuring the Customer Protection Program is explained to all employees;
- Ensuring the Customer Protection Program is implemented and accessible to all employees;
- Reviewing and updating Customer Protection Program related procedures;
- Ensuring that all concerned employees are trained;
- Ensuring that all escalated Customer Protection Program cases are duly analyzed and answered;
- Giving guidance, advice, and recommendations to management;
- Developing Customer Protection Breach detection controls;
- Ensuring the detection tools are in place;
- Conducting ex-post analysis and ensuring the investigations are conducted properly;
- Reviewing and Improving internal controls;
- Reporting on risk exposure to all concerned departments;
- Monitoring the evolution of risk exposure;
- Strengthening the setup on a regular basis based on confirmed cases and new trends;
- Taking disciplinary action toward the perpetrator (when applicable);
- Keeping the reports and documents received;
- Preparing periodic reports for the Board of Directors about the efforts towards Customer Protection Program to guide them; assist them in setting up the framework and to report any Customer protection breach (depending on the risk, it could be included in fraud risk committees, in compliance committees or included in operational risk committees);
- Implementing of all recommendations or findings issued by the audit department or any external review.

To enable the successful supervision of the Customer Protection Program, Risk or Compliance department must have enough independence from business lines to prevent from conflicts of interest and provide objectives, advices, and recommendations.

The Audit Function is responsible for:

- Providing assurance to the organization's board and senior management that customer protection risk is managed in an effective way by the organization;
- Reporting to the audit committee of the board of directors;
- Assessing independently the Customer Protection Program through periodic evaluations;
- Documenting the findings;
- Assessing the Customer Protection Program including (i) the procedure and policies, (ii) the authority and expertise of the designated Compliance/Risk Manager, (iii) and, the transactions monitoring and reporting;
- Assessing on a sample basis the quality of treatment of cases related to the Customer Protection Program;
- Ensuring that all concerned employees have performed the required trainings;
- Assessing the effectiveness of trainings;
- Performing review on a regular basis.

III. Approach for Customer Protection

Based on Principles of Financial Customer Protection' AA Exchange Company (Pvt.) Ltd.'s commitments are in the following sections.

PRINCIPLE 1 Equitable and fair treatment

AA Exchange Company should deal fairly and honestly with customers at all stages of their relationship, so that it is an integral part of the culture. Care should also be made, and special attention given to the needs of vulnerable persons and groups.

PRINCIPLE 2 Disclosure and transparency

AA Exchange Company should provide up to date information about products and services to customers. This information should be easily accessible, clear, simple to understand, accurate, not misleading and include any potential risks for the customer. It should include the rights and responsibilities of each party, including the mechanism for either party to end the relationship, as well as details of fees, pricing, and any potential penalties that the customer may incur.

PRINCIPLE 3 Financial education and awareness

AA Exchange Company should develop programs and appropriate mechanisms to help existing and future customers develop the knowledge, skills and confidence to appropriately understand risks, including financial risks and opportunities, make informed choices, know where to request assistance when needed.

PRINCIPLE 4 Responsible Business Conduct

AA Exchange Company should work in a professional manner for the benefit of customers during their relationship, where the Company is primarily responsible for the protection of the financial interests of the customer. AA Exchange Company should have a written policy on conflict of interest and ensure that this policy will help to detect potential conflicts of interest.

When the possibility of a conflict of interest arises between the Company and the third party, this should be disclosed to the customer.

PRINCIPLE 5 Protection of privacy /cybersecurity

Customers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used, and disclosed (especially to third parties). Company should have a written policy cybersecurity and ensure that this policy will help to detect potential security breaches and define the necessary IT security components (firewalls, antivirus updates…)

PRINCIPLE 6 Complaints handling

Customers should have access to adequate complaints handling mechanisms that are accessible, affordable, independent, fair, accountable, timely and efficient.

PRINCIPLE 7 Protection against fraud

AA Exchange Company should protect and monitor customers' funds through the development of control systems with a high level of efficiency and effectiveness to reduce fraud, embezzlement, or misuse.

PRINCIPLE 1: EQUITABLE AND FAIR TREATMENT

All customers should be treated equitably, honestly, and fairly at all stages of their relationship with financial service providers. Treating customers fairly should be an integral part of the good governance and corporate culture of all financial services providers and authorized agents. Special attention should be dedicated to the needs of vulnerable groups.

Employees must give priority to serving the interests of customers, without giving unfair preference to any individual or group of individuals. They must ensure that customers are adequately informed, notably regarding the risks involved in proposed transactions whenever the latter do not have extensive experience in dealing with such transactions.

Confidentiality

Internal information about AA Exchange Company should be considered confidential. Some information is of course publicly available, but much is not and should be treated confidentially...

All information with respect to a customer's affairs, whether sensitive and whether publicly available, are confidential. It should never be discussed with anyone outside the company except as may be required in the performance of services to that customer. The Company's secrecy laws demand stringently restrict the disclosure of information about its customers, including the simple fact that the person is a customer of AA Exchange Company.

Employees have a positive duty to safeguard all confidential information obtained in the course of his or her employment with the company. All information received as an employee, regardless of its source or nature, should only be used for the purpose for which it is provided. The information should not be used for any other purposes and it certainly should not be used for the personal benefit of the employee. Collected information can only be shared with the concerned customer only and not to any other non-authorized parties

Discussions of work in the presence of third parties whether the other people work outside or even in another department could lead to inadvertent disclosure of confidential information.

- Do not discuss confidential matters in lifts, corridors, or other shared facilities in the building.
- Avoid discussing confidential matters in public places such as taxis, restaurants, etc...
- If it is necessary to discuss office matters in a public place, care should be taken to avoid mentioning any customer's name or other details which might reveal a customer's identity or information about a particular transaction.
- Do not leave confidential documents lying unattended on your desk, particularly overnight or at lunchtime. For security and confidentiality reasons each employee is responsible for closing his/her offices' drawers before leaving the office at the end of the day.
- Preliminary draft documents or any other kind of document, not being retained should be shredded.

- All collected information and documents should be erased or shredded at the end of the record keeping period.

In the event of any problems arising over breach of confidentiality, or in the event of a perceived or potential breach of confidentiality being foreseen, the Compliance Department should be immediately notified.

Exceptions

AA Exchange Company has a general duty of confidentiality towards a customer except:

- When the disclosure is imposed by the relevant authority (such as LEAs or any other authorized body).
- When disclosure is made with the written consent of the customer.

PRINCIPLE 2: DISCLOSURE AND TRANSPARENCY

Company should provide customers with key information regarding the customer's fundamental benefits, risks, and terms of the product. They should also provide information on conflicts of interest associated with the authorized agent through which the product is sold.

Customer rights

AA Exchange Company treats its customer fairly and in accordance with the best industry standards as well as in accordance with local regulations. Service terms and conditions are displayed to the customers in order to ensure that customers know what their rights are. These terms and conditions cannot go against the local regulations, standards, and best practices in terms of customer management should be implemented.

Therefore, signatures need to be collected for all transactions on the copies of transaction receipts and upon the receipt of any contracts related to product and services provided by the company. These signatures may be used as a proof that the customer accepts the terms and conditions.

All required information to customers must be disclosed regarding each transaction and each terms and conditions mentioned in any contract including information related to fees charged and any additional regulatory.

Customer Documentation and Terms and Conditions

Standard form customer documentation has been adopted by AA Exchange Company and should be used.

Up to date terms and conditions for products and services should be provided to customers, through the channels available from company and in accordance with the customer's preference, and detailed either by way of a general terms and conditions booklet or by individual brochures.

Customers should be encouraged to read these terms and conditions before committing to a product or service.

The Company should communicate any changes in terms and conditions in advance of any such changes being implemented.

All terms and conditions should be written in clear and understandable language, in a manner that is not misleading and provided to the customer in local language, with a translation available in English if requested.

The Company should include specific warning statements in all terms and conditions, application forms and advertisements, clearly stating the potential consequences for the customer in not meeting the product or service conditions as agreed in the application form.

Customer's Understanding of The Risks

Employees in direct contact with customers should not recommend a transaction for any customers unless they are certain that the customers have the capability to understand and evaluate the nature, terms, conditions of and the risks involved in the concerned transaction. This is particularly important when dealing for private customers or if recommending a highly

speculative, an illiquid or a derivative transaction to a customer. Full disclosure of all charges should be made to all customers. In addition, employees must ensure that the proposed products or services match with the needs and objectives expressed by the customer.

PRINCIPLE 3: FINANCIAL EDUCATION AND AWARENESS

Appropriate mechanisms should be developed to help existing and future customers develop the knowledge, skills and confidence to appropriately understand risks, including financial risks and opportunities, make informed choices, know where to go for assistance, and take effective action to improve their own financial well-being. The responsibilities of customers will be supported by on-going customer education and awareness programs from the company. Customer responsibilities include the following:

Being honest with the information provided. Customers must always give full and accurate information when filling in any documents and must not give false details or leave out important information.

Carefully read all information provided by the company. When submitting an application, Customers should receive full details on the obligations for the applied service or product. Customers must ensure that they have access to the details of their obligations, that they understand them and that they can comply with them.

Ask questions. It is important for customers to ask questions to the Front Line Associates (FLAs) about anything that is unclear or a condition that they are unsure about. The staff will answer any questions in a professional manner to help them in their decision making.

Know how to make a complaint. Customers can be proactive in using this service and knowing how to escalate their issues to higher levels, if appropriate. Company will provide them with details on how to complain and the timeframe for their response.

Use the product or service in line with the terms and conditions. Customers must not use the product or service, except in accordance with the associated terms and conditions, and after making sure of their complete understanding.

Avoiding risk. Customers must not purchase a product or service where they feel that the risks do not suit their financials situations. Some financial products or services carry risks and company should clearly explain these to them e.g. remit funds to unrelated beneficiaries for the purpose of visa/lottery or others scams.

Apply for products and/or services that meet your needs. When making a request for a product or service, customers should make sure that it suits their needs. They should disclose all required information for KYC and additional supporting documents for CDD/EDD with Front line associates and compliance team to ensure the decision is based on their ability to meet their requirements for offered the product or service.

Report unauthorized transactions to Company if customers have discovered unauthorized transactions on their account, staff should report this to Company's Compliance/AML department immediately for suspicious transaction/activity reporting to regulatory body.

Not disclosing personal information. Under no circumstances should customers provide any details or other sensitive personal or financial information to any other party.

Talking to Company when encountering service difficulties. By talking to Company's officials, customers can discuss possible service arrangements that will enable them to fully discharge their responsibilities.

Updating information. Customers should update their personal information, including contact number, email and address information etc., so that it is updated continuously and when so requested by the company. Customers are responsible for failing to provide all relevant information to the company.

Contact details. Customer must use their own contact details (regular mail, phone numbers and email) when giving contact details to the company and must not use other friends' or relatives' contact details which can expose their financial information to others.

Not signing uncompleted forms. Customers must make sure all the required fields are completed in a form that is presented to them for signing or initialing and must not sign empty or partially completed forms (in Outward remittances / FTT).

Reviewing all documents. Customers must review all their documents before signing them to ensure no errors are made in the account number or amount. Their signatures are an approval and agreement of the document content.

Keeping copies of documents. Customers must keep all documents (transactions receipts) in a safe place that are provided to them by the company for their record and use (where required). Company should provide them with a copy of signed stamp receipts (by considering the regulatory requirements).

PRINCIPLE 4: RESPONSIBLE BUSINESS CONDUCT

Values

AA Exchange Company a Financial services provider and authorized agent, aims to work in the best interest of their customers and be responsible for upholding financial customer protection.

AA Exchange Company is committed to establish and maintain a culture based on trust, expertise, and respect for all of business relationship's legitimate interests. These commitments take the form of several actions all sharing the objective of continuous improvement in the quality of products and services provided. The company uses the expertise and experience to offer appropriate products and services for customer's situation and requirements and to bring their plans to fruition or anticipate financing needs; advise and inform them, considering their level of expertise.

It is necessary to emphasize the importance of attached standards of honesty and integrity with the company. These are criteria which all employees are asked to follow throughout the course of their employment.

Employees are expected to act in a professional, diligent, and loyal manner towards other members of their team as well as towards company and its customers, in accordance with laws and regulations in force.

Access to customer information

AA Exchange Company should ensure that the personal information of customers can be accessed and used by authorized employees only. This is to ensure that access to customer's financial and/or personal information is for authorized employees only, whether on the job or after they have ceased working with the company.

Employee members who suspect money laundering or face questionable or irregular activities must report their suspicions immediately to the Company's Compliance Manager/MLRO.

Communication

Employees must comply with the principle of company secrecy and respect the obligation of discretion in order to protect business confidentiality. The circulation of confidential information must be limited to employee members on a need-to-know basis only.

Employees must scrupulously comply with the rules and regulations of the markets in which they operate and must not circulate false information, manipulate the price of a financial instrument, disclose inside information or engage in any other activity which could impede or distort free matching of supply and demand and equal access to information. Only employees who have been granted the requisite authority may validly commit. Relations with supervisory and government authorities should be only conducted by the persons duly authorized by the company.

Employee must ensure that they will not engage the company or speak as representative of the company for any non-professional activities or responsibilities that he or she may exercise outside such as involvement in a politic party, association or any other personal activities. For public speeches and activities, employees must ensure to mention that he or she speak on his or her behalf only. Any doubt must be escalated to the Compliance Manager.

Conflict of interest

Employees should avoid situations generating conflicts of interest in which company or one of its employee members may be suspected of not acting in an entirely independent manner. Conflicts of interest must be resolved fairly and with the utmost neutrality so as never to place customers at a disadvantage.

Employees should take care not to generate conflicts of interest between their professional and their outside activities. Employee are prohibited from accepting or offering any gifts to customers or official bodies or their representatives except as permitted by the prevailing policy. Employees must avoid their own interests or those of their immediate circle entering into conflict with the company's interest. Everyone must avoid taking any financial interest in a competitor, supplier, or customer without prior permission in writing from their line management and the Compliance department. Employees must refrain from maintaining personal relationships with customers, partners and suppliers which could compromise their professional duties. Where there is any doubt about transactions or situations with respect to this policy or any applicable Instructions, the concerned employee should seek advice from his/her line management and the Compliance department.

PRINCIPLE 5: PROTECTION OF PRIVACY /CYBERSECURITY

Customers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used, and disclosed (especially to third parties). The mechanisms should also acknowledge the rights of customers to be informed about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data.

Safeguarding information

AA Exchange Company must safeguard non-public personal information. Employee may only ask for and collect the personally identifying information that is necessary to complete the transaction. Employees shall protect customers' personal and private information, in accordance with applicable laws and regulations, to prevent unauthorized access, use, and disclosure. Employees should implement procedures for safeguarding customer information.

Employees must protect customers' personal and private information. All documents that contain customers' private and personal information will be stored in a secure location. If employees wish to legally discard any related documents, the documents must be destroyed prior to disposal after management approval.

Company's Management is required to implement controls to protect its hardware / software to ensure data protection and security. It is direct responsibility of the company to protect customer data and maintain the confidentiality of the data, including when it is held by a third party.

Management will provide a safe and confidential environment in all its delivery channels to ensure the confidentiality and privacy of customer data and should have sufficient procedures, system controls and checks and employee awareness to protect customer information and to identify and resolve any causes of information security breaches, where they may occur in the future.

Compliance team is required to maintain appropriate safeguards for nonpublic personal information, including having written policies in place regarding the collection and disclosure of customer information considered to be "nonpublic personal information" and designating an employee or employees to coordinate information security program.

Regarding the use of external tools (to monitor transactions for examples), internal policies should be implemented to ensure an appropriate security protocols with regards to customer's information.

Tips

- Avoid loudly referencing identification data such as addresses, telephone numbers, etc. where others can hear what you are saying.
- Avoid using instant messaging, personal emails or web browsing on computers used to provide any products or services.
- Individual logins and password for authorized users are used and not shared with other employees
- Never show the system monitor screen to any customer through computers facing away from public

- Appropriate anti-virus and Firewall software must be installed and set to be automatically updated.
- Any notes, forms, logs, or other documents containing a customer's nonpublic personal information must be shredded before disposing of the documents.
- Encrypt or alter personal data to ensure they cannot be linked to a customer.
- Process on a regular basis the maintenance of the systems to ensure an ongoing confidentiality, integrity and availability of the personal data.
- Perform tests to assess the effectiveness of the system and the security measures.

PRINCIPLE 6: COMPLAINTS HANDLING

Management should ensure that customers have access to adequate complaints handling and redress mechanisms that are accessible, affordable, independent, fair, accountable, timely and efficient. Such mechanisms should not impose unreasonable cost, delays, or burdens on customers. In accordance with the above, management should have in place mechanisms for complaint handling and redress related to MTO's and Front Line Associates. Recourse to an independent redress process should be available to address complaints that are not efficiently resolved initially "internal dispute resolution mechanisms". At a minimum, aggregate information with respect to complaints and their resolutions should be made public (where necessary).

Error

Company is not entitled to benefit from any amounts due to an error, the sum should be returned to the affected customer's account without delay and without waiting for the customer to register a claim.

Where the Front Line Associate discovers an error or is informed of an error by a customer making a complaint or a claim, then FLA shall should refund all other customers who are proven to be affected by a similar error. This should be completed within sixty (60) business days of the original error being identified. Company should issue a communication to all affected customers, advising them of the error and the steps being taken for corrective action, including the amount of the refund to the customers' accounts.

Company should ensure the continuity of systems to meet the customers' needs at all times, and to provide alternatives when a defect or malfunction occurs.

On conclusion of a complaint or error investigation, or on receipt of an instruction from a higher authority, any refunds or monetary compensation due to a customer should be credited to the customer's money transmission account within five business days.

In certain exceptional circumstances when a longer period may be required, the customer should be advised of the expected time for crediting of the amount due.

Complaints

Customer complaints and disagreements should be dealt with promptly and fairly. It is imperative that all persons who make any complaint be treated politely and with courtesy.

All complaints from customers, whether verbal or in writing, should be reported promptly to the respective Department Manager (Operation Department). If the matter involves a purely administrative matter and there is no suggestion of any misconduct, the Department Manager should endeavor to resolve the matter promptly, efficiently, and courteously. If the complaint cannot be promptly remedied, the Department Manager should advise the Compliance Manager.

Customer's refunds

Company must have a clear internal policy to manage refund requests from customers or other parties concerned by a product or services provided. The procedure must detail the

process, the investigations to do, the employees in charge and the direct line the concerned parties must use for these requests.

PRINCIPLE 7: PROTECTION AGAINST FRAUD

Fraud Risk Management Framework at AA Exchange Company shall have the following mechanisms: Understand the fraud and misconduct risks that can undermine the business objectives.

1. Determine whether anti-fraud programs and controls are effective in reducing instances of fraud and misconduct.
2. Gain insight on better ways to design and evaluate control s to prevent, detect and respond appropriately to fraud and misconduct.
3. Reduce exposure to corporate liability, sanctions and litigation that may arise from violations of law or market expectations.
4. Achieve the highest levels of business integrity through sound corporate governance, internal control and transparency.

Identification of the risks

A key component of building a strong strategy starts by identifying the areas of risks. A risk assessment needs to be built and reviewed on a regular basis (at least once a year) to list the potential fraud risks based on:

- trends identified by local regulator and international standards (examples: ACFE, EU regulations, US regulations);
- Historical data (fraud cases identified in the past).

For each external risk identified, Company's nominated Fraud Manager must liaise with the concern manager and jointly address clear actions to mitigate the risk identified. For example, if an area of risk is identified with financial transactions, the manager in charge of this product should be involved in the definition of the anti-fraud program to prevent this specific risk.

An effective, fraud risk management framework is focused on three objectives:

Prevention:

- Ethical culture;
- Allocation of responsibilities;
- Controls designed to reduce the risk of fraud and misconduct from occurring in the first place;
- Staff training and awareness;
- Customer awareness;
- Internal controls processes and systems.

Detection:

- Fraud indicators;
- Escalation mechanism including the use of the hotline set and accessible for all employees;
- Teller awareness to detect fraud through challenging questions around purpose of transaction and relationship sender/ receiver;
- System controls designed to discover fraud and misconduct when it occurs.

Management

- Investigations;
- Risk mitigation;
- Legal actions;
- Controls designed to take corrective action and remedy the harm caused by fraud or misconduct;
- Information to management.

IV. Record Keeping

Types of records and documents that should be kept :

1) Records and documents related to the transactions made with Customers provided they include enough information to enable identification of details of each transaction separately
2) Reports about potential breach case and evidence that they had been reviewed .
3) Records and documents related to reports kept by the designated Compliance/Risk Manager.
4) Records related to training programs; must include information about all programs attained by the employees in the field of combatting fraud, names of trainees, sections and departments where they work, the content of the training program, its period and the training centers performed the training at home or abroad.
5) Record of all internal and external audits perform.
6) Record of all reporting to management, Board of Director and authorities.

Conditions to be followed for Records retention

1) Keeping all records, documents, and reports safely, and keeping reserve copies in another place
2) Keeping records and documents must be done in a way that enables quick and easy recovery of the documents, so that access to any information or information needed shall be precise and without delay

The retention Period

All record keeping and reporting documentation required by specific regulations will be maintained for a minimum of Ten (10) years and they will be made readily available to the regulator and/or representatives from other government officials upon legitimate request.

V. Independent review of the Customer Protection Program

In connection with the continued efforts to protect customer, meet regulatory requirements and apply international best practices, company always seeks to continuously enhance its Customer Protection Program. As part of this effort, it requires conducting a periodic independent review of its Customer Protection Program.

The purpose of the independent review is to evaluate the effectiveness of Customer Protection Program.

Independent reviews shall be documented in writing and they shall document the actions it has taken in response to any deficiencies identified by the independent review.

Independent reviews shall consider the adequacy of:

- written Customer Protection Program;
- authority and expertise of the company's designated Customer Protection Program responsible;
- employee training;
- transaction monitoring and reporting, including customer complaints, customer refunds, the filing of suspicious activity reports and/or referral of suspicious activity, when necessary; and
- Any other deficiencies related to the implementation of and adherence to the Policy.

An Independent Review is to monitor the effectiveness of the Customer Protection Program as required by local regulations and internal policies. The review also ensures that the company is operating in compliance with the local and country requirements as well as the internal policies.

The review is done either by Internal Audit or by External auditors.

As a reminder:

- An Independent Review is required by local regulator and must be done annually.
- The Independent Review will be conducted by a person or persons who are knowledgeable about the Customer Protection Program requirements that apply to current activities.
- The Independent Review cannot be conducted by the company's designated compliance officer or anyone that reports to him

Once the Independent Review has been completed and the report has signed by the reviewer, please keep/file/store it for at least 10 years.

VI. Appendixes

Appendix 1: Best Practices

Send side

- Ask questions in a friendly, non-threatening manner;
- If you suspect fraud, tell the customer that similar transactions have indicated fraud and that they should think twice before sending the money;
- If you suspect the sender is a victim of customer fraud, reject the transaction and report the incident to your Chief Compliance Officer.

Receive Side

- Ensure payee provides complete required and payout information;
- Refuse to pay the transfer if the receiver does not provide all the information;
- Closely examine identification presented and ask for a 2nd form of ID if the primary ID presented looks suspicious;
- Photocopy or Scan ID(s) presented if you suspect fraud;
- Report all suspicious activity of customers and colleagues to your supervisor and to the Compliance Department.

Appendix 2: Definition of fraud

Fraud can be broadly defined as an intentional unlawful act or omission of an act of deceit to obtain directly or indirectly, and undue tangible or intangible and unjust/illegal advantage for its own benefits or for the benefits of a third party. For the purposes of the policy, fraud shall include but is not limited to, internal fraud, external fraud and attempt or aborted fraud as defined below.

<u>Internal frauds</u>

Frauds directly or indirectly (through hidden relationships such as relatives) linked to an employee targeting any victims either internal employees or external (Partners, Customers, etc...); including those perpetrated by an employee outside the performance of his/her professional activities; that lead to any damage including, but not limited to AA Exchange Company's assets, reputation, Business relationships, losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party. Internal fraud also includes:

- Market abuse**:** the concept of market abuse typically consists of insider dealing and market manipulation of the financial markets:
    - Insider trading: In this type of scenario, generally a person who is having some very important information that is usually not publicly available, uses this information for his/her own personal gain.
    - Market manipulation: A person may knowingly hand over some false or misleading information to influence the prices of a targeted share.

- Fraud related to situation involving a **conflict of interest**: A conflict of interest arises where an employee has some other interest that could materially interfere with their duty to act impartially in the decision process. All employees are required to disclose any potential or confirmed conflict of interest once identified. A conflict of interest affects, or can be perceived to affect, a person's independence, objectivity or impartiality. It occurs when an individual is subject to two coexisting interests that are in direct conflict with each other.

Examples:

- Accepting or offering a bribe or accepting gifts or other favors under circumstances that might lead to the inference that the gift or favor was intended to influence an employee's decision- making while serving the company;
- 'Off the books' accounting, or making false or fictitious entries;
- Knowingly creating and/or distributing false or misleading financial reports;
- Paying of excessive prices or fees where justification thereof is not documented;
- Violation of the company procedures with the aim of personal gain or to the detriment of the company;
- Willful negligence intended to cause damage to the material interest of the company; and a dishonorable or reckless or deliberate act against the interests of the company.

External Frauds

We distinguish three main types of external frauds:

- Frauds targeting directly or indirectly to company such as (list non-exhaustive):
    - Theft or misappropriation of assets owned or managed by the company;
    - Customer's Submitting false claims for payments or reimbursement;
    - Cyberattacks;
    - Blackmail or extortion.
- Frauds targeting company's customers and processed using any product or services such as criminals operating schemes or scams to persuade customers to send money for specific purposes that might sound financially appealing to the customer, but, are only ways to convince customers to part with their money. Most customer fraud involves the perception on the part of the victim that they will receive some sort of financial gain or that they are helping a friend, relative or loved one. In short, customer fraud is the potential or actual theft of funds from a customer by means of deceit, trickery, or manipulation.
- Fraudulent identification and use of falsified documents.

Attempted or aborted fraud

Fraud aiming at an end up advantage that has not been attained. Any attempted fraud should be considered and treated as a confirmed fraud.

Example of situation: *An employee receives an email that appears to be from the CEO of an company's business relationships. The employee does not see that the CEO's address has been compromised with a fake look-alike email domain and processed the payment. The employee contacts the customer to confirm the payment and noticed the fraud case. By quickly reporting the incident, the employee was able to recall the funds successfully*.

Appendix 3: Fraud Red flags

Indicator of fraud induced transactions send side

Below are some of the potential behavior al and transactional indicators needed to be familiar with that will assist us to detect if customers may be victims of fraud.

- Sender who may seem apprehensive or confused, especially elder and dependent adults.
- Sender who seems overly excited to send money.
- Sender who expresses concern about sending money for an emergency.
- Sender who seems excited or anxious about receiving a large sum of money or "once-in-a lifetime deal".
- Sender who may be sending money for the first time and ask questions about the process. Sender who sends multiple transaction s in a single day or over the course of a few days.
- Sender who wishes to protect or delay their money transfer by using a test question. Sender wants payout delayed.
- Sender is sending to someone he/she doesn’t' know. Sender asks about changing payee name.
- Senders who send to a famous person, or fictional character.
- Senders who mention prize, lottery, rental, eBay, grandchild, fiancé.
- Sender writes unusual instructions on send form: "do not pay until instructed". Senders who may not fit our usual customer profile.
- Customers who use the same name for the sender and receiver

Indicator of fraud induced transactions receive side

For every person who is victim of customer fraud, there is fraudster on the receive side of the transaction, picking up the money.

Below are some of the potential indicators needed to be familiar with that will assist us to detect fraud induced transactions on receive side?

- An individual repeatedly picks up transactions from multiple senders in multiple locations (states/countries).
- An individual attempt to pick up a transaction in a country other than where it was intended to be sent.
- An individual receives multiple transactions & immediately wants to send all the funds to a new location.
- There does not appear to be a family connection between the receiver & the sender (different last names for example).
- There does not appear to be a business purpose for the transaction.
- There are so many senders that is seems unlikely that the receiver knows that number of people

Company's designated Fraud Manager must be aware of all types of common red flags.

Appendix 4: Fraud Prevention

Fraud prevention consists in implementing a strategy to stave off internal and external frauds. As technology means and the technics used by fraudsters evolved quickly, a strong fraud prevention strategy updated on a regular basis is essential.

The key components of the strategy are:

- An ethical culture and awareness among the company.
- A well-planned segregation of duties;
- Efficient trainings;
- Strong internal controls and systems (processes and tools).

Ethical culture and awareness:

Ethical behavior: Preventing major frauds requires a strong emphasis on creating a workplace environment that promotes ethical behavior, deters wrongdoing and encourages all employees to communicate any known or suspected wrongdoing to the company's anti-fraud designated Manager. Senior managers may be unable to perpetrate certain fraud schemes if employees decline to aid and abet them in committing a crime. A strong ethical culture among employees is the best defense against internals frauds. In addition, and to ensure the high importance of the ethical behavior, job descriptions of all employees must include a section dedicated to ethical behavior with clear objectives assessed on a yearly basis to determine their compensations.

Abiding to the company's Global Ethics policy: All employees must read and understand the company's Global Ethics policy based on the company's core values, which gives clear guidance on behaviors and actions that are permitted and prohibited. The Global Ethics policy describes how employees should seek additional advice in case of doubt regarding a misconduct or a wrongdoing and how they must communicate concerns about known or potential wrongdoing. The implementation of a hotline is crucial and must be known by all employees. This hotline could be a company's website, a phone number or an email. It is crucial to create an environment in which callers feel sufficiently confident to express their concerns openly. Hence, an Anti-fraud designated officer or the Compliance Manager must include the protection of all callers from retribution in the policies and procedures to ensure that employees will use of this hotline when required.

A similar hotline must be used to enable the business relationships (partners, customers and others) to communicate concerns about known or potential wrongdoing or if they are victim of a fraud performed through company's systems or through any its products or services provided. Company's Fraud designated Officer must ensure that all business relationships know the existence of this hotline and how to access and use it.

Segregation of duties and management approvals:

AA Exchange Company must include is the procedures a clear segregation of duties including, at least, authorizations for specific tasks (transaction above a certain threshold or the use of a risky product for example), recording or reporting of transactions and for setting up management and control systems which comply with local requirements and international standards. For example, some fraud risks relating to receipt of funds can be eliminated or mitigated by centralizing that function, where stronger controls can be more affordable. It is important to communicate both internally and externally that the organization has a

coordinated approach towards combatting fraud to deter internal and external fraudsters. For example, the risk of sales representatives falsifying sales to earn commissions can be reduced through effective monitoring by their branch manager, with approval required for sales above a certain threshold.

Trainings

An important part of the company's Anti-Fraud Compliance Program is employee training.

One of the key components of an effective Compliance Program is employee training, both before starting to conduct transactions as well as periodic ongoing training based on the complexity and employee turnover related to your business:

- Every Compliance Officer (CO) and employees who interact with customers must have initial and ongoing AML and Anti-Fraud Training:
    - For new employees, Anti-Fraud training needs to be provided before the employee starts processing transactions. Before conducting transactions, employees should be required to review all the information in the Training Guide and sign a copy of the Acknowledgment Form that will be retained in their personnel file or the business's files.
    - Refresher training should take place at least every two years or more frequently as required by local laws and regulations.
    - Additional training should be provided regularly to all employees based on, but not limited to, changes in government regulations, Anti-fraud Program requirements, or procedures and policies.
    - Dedicated training related to the Anti-fraud related Officer needs to be provided to compliance employee representative.
- Company also provide additional employee training in the event a performance issue related to the anti-fraud program is identified.

To be considered adequate and sufficient, employee training must:

a. Explain internal policies and procedures;
b. Identify how and where training records are filed and permanently kept;
c. Explain regulatory reporting for all types of products and services offered (e.g., Money Transfer, Foreign Currencies Sales/Purchase, FTT, Branchless Banking), as applicable;
d. Explain fraud prevention and detection regarding Agent and Customer fraud;
e. Explains common fraud types, how to identify them, and how to escalate them once identified;
f. Explain recordkeeping and record retention requirements (including document destruction policy);
g. All relevant transaction processing requirements;

h. These may vary based on region;

i. Explain how to identify acceptable forms and verify customer identification;

j. Stresses importance of correct data collection and data entry as well as data integrity;

k. Have adequate instructions for handling customer complaints;

l. Explain the notions of conflict of interests and market abuse and the penalties they could face in case of attempt or confirmed fraud;

m. Ensure that all employees acknowledge and abide with the company's Global Ethics policy;

n. Ensure that all employee knows the existence of the hotline and in which case it must be used;

o. Explain the potential area of risks which could lead to a fraud against the company such as falsified domain name, falsified link, the use of company's laptop for a purpose unrelated to the professional activity;

p. Ensure that employees are aware that an efficient system (processes and tools) is in place to detect internal and external frauds.

Internal control systems (tools and processes)

Company's anti-fraud program must include an operational internal controls and systems to mitigate the risks identified. All operating units in coordination with the fraud designated officer must develop and review on a regular basis (at least once a year) a system of controls to:

- Ensure the assets and the records of the company are adequately protected from loss, destruction, theft, alteration, or unauthorized access;
- Check the systemic verification of operations for each area of risk identified;
- Check the efficiency of the detection of internal and external fraud.

The system must be assessed by the Audit function periodically and the authorizations and accesses to this system must be reviewed on a regular basis especially after a system upgrade and when the organization change.

Essential rules to apply

To tighten security at your branch location and to help prevent your branch location from becoming a victim of fraud, NEVER perform any of the following actions:

- NEVER send a money transfer transaction without collecting funds.
- NEVER enter any information into the Company system based on an incoming phone call.
- NEVER agree to a PC support connection unless you have initiated contact with Company or your corporate office regarding an issue with your PC, even if the caller states they are from Company or your network's technical services.
- NEVER download software from an unknown source or insert a CD/USB provided to you into the PC providing Company services.
- NEVER enter a test/training transaction into the live system.

- NEVER return or make a call to Company using a telephone number supplied by the caller.

Take these technical actions to protect the branch location from fraud:

- PCs with the company should run industry supported software only and must be upgraded/patched in a timely manner when prompted. Ensure adequate anti-virus, antispyware and firewall programs - set an auto-update/ auto-run for daily protection.
- Do not run external email capabilities.
- Disable USB ports, floppy disks and CDROMs on PCs used to provide Company services.
- Set designated hours of operation in the Company system so that the money transfer system is not active after hours. Shut down the PC after the designated hours of operation.
- Employees should lock PCs when leaving their workstations.
- Delete the Operator IDs for any resigned or terminated employees.
- Operator IDs and passwords should never be shared with anyone, including other employees or anyone requesting passwords over email or text. Passwords should be changed every 90 days.

Appendix 5: Fraud Detection:

Fraud can be detected at any level within the company, and the following will apply in the reporting of suspected internal fraud:

- An employee or other person who suspects that fraudulent activity is taking place should, in the first instance, report the matter to their line manager;

- If an employee does not feel comfortable raising a matter with their line manager - due to the nature of the concern, its seriousness, or for some other reason - they can raise it immediately with a Senior Auditor and/or a member of the management team.

The main means to detect frauds are the following:

- Business relationships' complaints;
- Human vigilance and transactional controls;
- The internal monitoring systems implemented to detect internal and external frauds (could be through reports or a dedicated tool).

<u>Business relationships' complaints</u>

The complaints are an extremely important source of knowledge. Each complaint must lead to an investigation and must be answered in a timely manner. In case of confirmed fraud, company's designated Fraud Manager must understand the deficiencies, update the setup (if applicable), take relevant actions in case of the fraud should have been detected whether by an employee or by the detection system (tool or reports).

The complaints and the investigations must be reported to the management and the law enforcement (if required) and duly recorded including the detailed complaint, the analysis and all documentary evidence during at least 5 years (or more if required by the local regulator).

Human vigilance and transactional controls

All employees directly or indirectly in contact with customers must be trained to ensure they are aware of the potential indicators of frauds. Human vigilance and transactional Controls are performed daily:

- By paying an attention in customer's behavior (occasional or not);
- By knowing customers;
- By escalating each ethical misconduct or internal fraud identified to the company's designated Fraud Manager;
- By escalating for further analysis and refusing to process any transaction which may be fraudulent.

Ex-post analysis

Ex post transaction monitoring is performed through a rule-based formula applied to historical transaction data. The purpose of ex post transaction monitoring is to detect any pattern/situation deemed as unusual that cannot not be detected by employees' vigilance or complaints received. The designated Fraud Manager must

- ensure that the ex-post monitoring detects both internal and external frauds;
- Create and test the rules to ensure their efficiencies;
- Review the rules on a regular basis to ensure their relevancies;
- Create additional rules when a confirmed fraud occurs and could not have been detected by the ongoing monitoring (Employees and detection tool) if applicable.

For example, the ex-post monitoring could include (list non-exhaustive) the detection of one-to-many and many-to-one activities including employee's accounts to flag for example employees taking in multiple account a very small amount from the customer which may not be detected.

Periodicity of the monitoring

To ensure the effectiveness of the controls, the ex-post monitoring should be run at least once a month.

Appendix 6: Fraud Management

It is crucial to ensure that all escalated incidents related to potential frauds are duly analyzed. For incidents linked to Compliance issues, the incident must be escalated to the designated Fraud Manager and the Compliance Manager. The management of internal and external fraud must include at least the following:

- the analysis of the events: collection of proof elements and identification of any failure of the internal monitoring framework;
- the settlement of collective and individual responsibilities;
- the formulation of corrective measures to strengthen the setup;
- the determination of punitive action (when applicable);
- Correlatively and in coordination with the concerned departments, the assessment and the management of the other consequence of the fraud:
    - on the financial statement of the company;
    - on the reputation of the company;
    - on the internal and external communication;
    - on the need to report to the regulators, law enforcement authorities, boards of Directors and Boards committees;
    - on its Business Relationship with the concerned involved party(ies) (if external) or employee(s) (if internal);
    - In terms of administrative, civil, criminal or labor proceedings;
    - In the most serious cases of fraud, a crisis committee could be organized at the initiative of the company designated Fraud Manager.

All attempt or confirmed fraud cases must be escalated and reported to the Management and the Board of Directors.

<u>Reporting a suspected fraud</u>

Reporting fraud according to the following procedure is mandatory for any employee who suspects that a fraud has occurred. Persons who cover up, obstruct, or fail to report (or monitor) a fraud that they become aware of, or ought to have been aware of, may be considered to be an accessory after the fact and may be subject to the company disciplinary code which could involve act ion up to and including dismissal. Persons who threaten retaliation against a person reporting a suspected fraud shall be subject to the disciplinary code which could include action up to and including dismissal or prosecution or both.

Great care must be taken in dealing with suspected dishonest or fraudulent activities to avoid:

- Alerting suspected individuals to an investigation underway;
- Treating employees unfairly; and
- Making statements that could lead to claims of false accusation s or other charges.

Details of the incident, facts, suspicions or allegations should not be discussed with anyone inside or outside the company unless the company investigating team specifically directs this. In particular, the matter should not be discussed with the individual suspected of fraud.

Concerns may be reported verbally or in writing. Where a concern is raised verbally the following steps are to be taken by the employee raising the concern to ensure that the concern raised is acknowledged by the recipient as received in the manner intended by the employee.

These steps are to ensure that the recipient is clear that what is intend as a concern about suspected fraud is not construed by the recipient as a passing or casual comment.

- The employee raising the concern sends a written communication to the recipient. The written communication confirms:
  - the fact that a concern about suspected fraud was raised (details of the suspected fraud need not be included, just the fact that a concern is raised);
  - that a written acknowledgement from the recipient to the employee is required.
- The recipient responds with a written communication acknowledging receipt of the concern.
  - Once a report of suspected fraud is made to a supervisor/ manager, that person is required to pass that information promptly to his/ her Head of Division;
  - A Head of Division, Director or member of the Operations/ Audit Committee on receipt of a report of a suspected fraud are required, in turn, to report the matter promptly to the Auditor.

Investigation of alleged fraud

AA Exchange Company's designated Fraud Manager must establish and document a fraud investigation's protocols taking into consideration local regulations regarding employee's and business relationships' rights. Each investigation must be duly documented and recorded for at least 5 years (or more if required by the local regulator).

Examples of actions after confirming a fraud case:

- Defining new processes or additional controls;
- the settlement of collective and individual responsibilities;
- the formulation of corrective measures to strengthen the setup;
- the determination of punitive action (when applicable).

Appendix 8: Responding to Customer Fraud

Responding to Customer Fraud - Send Side

If you suspect customer fraud on the "send side" of the transaction, what should you do? Know Your Customer by asking questions if you are suspicious about the activity. For example: "Do you know the person you're sending money to?"

- "Did you verify the situation with another family member before sending emergency money to the person who contacted you?"
- "Are you sure the person who contacted you is really in need?"
- "Did you play the lottery or sweepstakes? Did you purchase a ticket or enter a drawing?"
- "Did you initiate the contact with the person you're sending money to or did they contact you?"
- "Are you sure the person you're sending money to works for the company they claim to represent? Have you verified that it is a reputable company?"
- "What is the purpose of the transaction?"

If you believe that the customer may be a victim of customer fraud, DO NOT process the transaction. Report customer fraud.

Cooperate with customer fraud investigations.

Responding to Customer Fraud - Receive Side

If you suspect fraud on the "receive side" of the transaction, what should you do? Know your customer by asking questions if you are suspicious about the activity. For example:

- "What is the purpose of the transaction and relationship with sender?"
- "How do you know the senders?'" "What line of business are you in?"

If you believe that the receive customer may be a perpetrator of customer fraud, DO NOT process the transaction.

- Tell the customer that there is a problem and he/she will need to contact sender. Immediately contact Chief Compliance Officer by phone to report the fraud incident.
- Cooperate with customer fraud investigations conducted by Compliance Department.
- Provide all the details/ documents collected and submit Fraud Incident Reporting Form to Chief Compliance Officer.

Special cases of frauds involving employee

No investigation of an internal suspected fraud should take place until the Head of operation or auditor has been informed. The Head of operation or auditor, in turn, will determine who best to inform i.e. the owners, the Chief Operations Officer and Human Resources Head. Auditor must investigate all instances of suspected frauds reported to t hem.

The Auditor (except in any case involving his or her division) will take the lead when fraud investigations are being conducted. This will involve data collection, analysis and intervention, including the review of internal controls.

Data quality

The quality of the data is basis of a solid AML/CFT program. Altered or non-accurate data lead to (i) longer processes in monitoring customers (i) failure to detect unusual or suspicious activity (iii) failure to detect potential international or local sanctions (iv) failure to answer requests from authorities.

Company's employees must pay a particular attention regarding the correctness and the accuracy of the data input in MIS.

Additional controls could be added to ensure the reliability and the accuracy of the data.

Cooperation with Law enforcement and regulators

AA Exchange Company abide fully with local and international regulations this includes answering to any request received from local and international regulators. The compliance department in coordination with Legal department are in charge of establishing and implementing policies, procedures and internal controls to ensure that (i) the information and documents requested are provided in a proper format (ii) an acknowledgement of receipt is quickly sent (ii) the information requested are verified and accurate (iii) the answer is provided in a timely manner and should be in line with local regulator and internal policies.