Anti-Money Laundering Compliance and Compliance Oversight Policy in 2024

1. TERMS USED IN THE POLICY OF LEGAL AND REGULATORY COMPLIANCE IN THE FIELD OF COUNTERACTION MONEY LAUNDERING

Customer Service Officer - an employee of the Company engaged in drafting/concluding agreements with Customers and/or securing Financial Operations, who has been appointed by the Company to perform the duties defined in the regulations established for Customer Service Officers.

AML - Anti-Money Laundering.

A beneficial owner is any natural person who:

- Ultimately owns or controls (through direct or indirect ownership or control, including through bearer shareholdings) more than 25% of the shares or voting rights in the entity (in respect of any person other than a company whose securities are listed on a regulated market); or
- Oversees the management of the organization (in respect of all corporate entities)

In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any natural person who:

- Is ultimately entitled to or controls (whether the rights or control are direct or indirect) more than 25% of the equity or profits of the partnership or more than 25% of the voting rights in the partnership; or
- Otherwise exercises control over the management of the partnership

In the case of a trust, "beneficial owner" means:

- Any individual entitled to a specified interest of at least 25% of the capital of the trust property;
- With respect to any trust other than a trust that is created or operated solely for the benefit of persons falling within subparagraph (a) the class of persons for whose benefit the trust is created or operated;
- Any person in control of the Trust.

Business relationship - a relationship between a client and a company, which is established in the course of the Company's commercial and professional activities and which, at the time of establishment, has a long-term purpose.

Consumer/Customer - a natural or legal person or an association of such persons to whom the Company provides or who wishes to receive Services from the Company.

The company is FIRST CLASS PAYMENTS INC.

Compliance Department - the department responsible for monitoring and evaluating customers and reporting suspicious/unusual transactions within the scope of this AML policy and responsibility.

Conclusion - information that the Compliance Department/Customer Service Officer

must complete to ensure that all required legal audit checks have been completed correctly and in a timely manner.

CTF - Counter Terrorist Financing.

Rejected Customer List - A list of rejected customers maintained by the Company that includes customers whose business relationship has been terminated due to AML/CTF fraud, or breach of agreement, as well as customers who have been analyzed and cooperation with them was refused due to an unacceptable level of risk.

System - a complex of software and hardware tools of the Company for data processing.

Services - services provided by the Company.

Information Technology (IT) Department - the unit responsible for regular payment authorization checks and transaction monitoring.

Identity document - a document of state sample.

Internet site - a site on which the Client uses the Company's services.

State-issued document (with photo) - valid passport, national ID card, valid driver's license.

Suspicious Indicators List - a list of transaction suspiciousness indicators established and maintained by the Company.

Client - a legal or natural person who has expressed an interest in receiving services, or a person who has a Business Relationship with the Company and who distributes goods and services through Transactions.

MLRO (Money Laundering Reporting Officer) - a person who is appointed to oversee and is responsible for overseeing the Company's compliance with the Money Laundering Systems and Controls Regulations.

PEP (politically exposed person) - an individual who performs or has performed in the previous year important public functions, close relatives, family members of such natural person, as well as persons known to be closely related to the said natural person.

Questionnaire - an application form developed by the Company, which is used in accordance with the recommendations of the legislation and international standards and is filled in and sent to the Company by the Client wishing to establish business relations with the Company.

STR - suspicious transaction report in FINTRAC.

Management Board - the directors of a company who are individually or collectively responsible for the management and supervision of the company.

Suspicious Transactions - transactions that give rise to suspicion of money laundering and terrorist financing, or attempts to do so, or are related to other offenses.

2. GENERAL CONDITIONS

The Company faces the risk that criminals may use the system for money laundering and terrorist financing. In order to control this risk, the Company has implemented a valid anti-money laundering (AML) policy aimed at preventing money laundering and the financing of criminal activities by ensuring compliance with the requirements set out in the PCMLTFA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act) and FINTRAC (Financial Transactions Analysis and Reporting Center of Canada) regulations.

The purpose of the AML policy is to define the basic principles of the Company's activities to prevent money laundering and terrorist financing and to establish a system of internal control commensurate with the Company's operations in order to minimize reputational and financial risks.

The procedures contained in this policy apply to all of the Company's Clients.

This AML policy is developed in accordance with the PCMLTFA on Selected Measures Against Legitimizing the Proceeds of Crime and Terrorist Financing and the FATF (Financial Action Task Force) recommendation on AML and CFT.

The Company's Management Board is responsible for the implementation of this AML policy, allocation of sufficient financial resources, engagement of qualified employees, organization and supervision of controls.
At least once a year, the Company's Management Board reviews the implementation of this AML Policy, approves necessary actions, assigns responsible roles, and monitors the implementation of plans.

The Company's Management Board appoints one of its members who is directly responsible for monitoring AML/CFT legislation and implementing AML policy.

The purpose of the preventive measures taken by the Company is to:

- Analyzing the requirements of the Company's internal regulations and their actual implementation in order to identify deficiencies in the existing system or the work of employees
- Improvement of internal regulations, training of responsible employees

In addition to the Board and the MLRO, employees of the Company are also responsible for implementing the relevant aspects of this policy.

3. DUTIES, RIGHTS AND RESPONSIBILITIES OF MLRO

The Company has a designated Money Laundering Responsibility Officer (MLRO) who reports to the Board. The MLRO is responsible for ensuring that the Company complies with the AML/CFT requirements of the PCMLTFA and FINTRACK regulations.

3.1. CORE BUSINESS MLRO

MLRO's principal activities include, but are not limited to, the following:

- Organization, management and control of the Compliance Department
- Ensuring compliance the Company compliance with anti-money laundering and anti-terrorist financing legislation;
- Development and improvement of the Company's AML internal control system and coordination of its implementation, development of relevant documentation of risk management policy and risk profile in relation to money laundering and terrorist financing;
- Performing regular assessments of the Company's systems and controls to ensure

effective money laundering risk management;
- Maintaining communication with FINTRAC and providing them with information upon request, as well as notifying FINTRAC if there are any relevant changes in the Company;
- Ensuring that the Company collects information on unusual and suspicious transactions;
- Work with internal reports, including deciding whether to submit reports to FINTRAC;
- Taking prompt decisions to prevent the execution of a Customer's transaction if the transaction is related to money laundering or if there are legitimate grounds to suspect that it is related to money laundering;
- Establishing a framework for the practical application of a risk-based approach to preventing money laundering and terrorist financing;
- Organization of staff training on money laundering prevention, as well as provision of advisory assistance to the Company's personnel;
- Supervision of compliance with regulations regarding money laundering systems and controls;
- Drafting job descriptions (duties and responsibilities) for Compliance staff and assigning responsibilities to Compliance staff;
- Evaluating the effectiveness of the internal control system, taking into account additional risks that may arise as a result of the development of new technologies, at least once a year.

3.2. MLRO RIGHTS.

In the performance of its duties, the MLRO shall have the right to:

- In a timely manner receive necessary information to perform their duties;
- Represent Company in matters related to in matters related to combating money laundering;
- Issue binding instructions to the Company's personnel on all matters related to anti-money laundering.

3.3. MLRO LIABILITY

In the performance of their duties MLRO is also is responsible for:

- Timely performance of his/her duties;
- Developing a policy on money laundering procedures;
- Establishing and maintaining effective anti-money laundering systems and controls.

3.4. MLRO REPORTING TO THE BOARD

MLRO reports to the Board include:

- Annual Reports - Once a year, the MLRO prepares a report that evaluates the operation and effectiveness of the Company's system of internal controls in relation to managing the risk of money laundering. After reviewing the report, the Board considers and identifies any areas for improvement.

4. INITIAL LEGAL AUDIT OF THE CLIENT

4.1. FUNDAMENTAL DECISION

In order to prevent the risk of money laundering and terrorist financing, the Company agrees that the client review process consists of two stages:

- Examination of the information provided;
- Comprehensive review.

4.2. REVIEW OF THE INFORMATION PROVIDED

Before a Customer Service Officer can make any decision regarding the Business Relationship, the customer must first complete an application form on the Company's website or call the telephone number listed in the Company's manual or send general information to the e-mail address listed in the Company's manual.

4.3. FULL CONSIDERATION

The customer service officer must ensure that the customer's activities are not included in the list of unacceptable activities (Appendix 1)

Customer Service Officer:

- Must ensure that the Client/beneficial owner/legal representative is NOT on the Rejected Client List;
- Must ensure that the Client is fully capable of acting;
- Must ensure that the Customer provides the services / declared transactions (Appendix 5).

If in doubt, the Customer Service Specialist may investigate further.

If publicly available information suggests or the Customer Service Officer subjectively believes that a potential Customer requires a license, special permit and/or registration with a competent authority to conduct business, the Customer Service Officer should ask the Customer to provide the necessary license or special permit for certain business activities. The Customer Service Officer should also verify the Customer's registration with the competent authority or understand why licensing/registration is not required.

4.4. FINAL DECISION

After reviewing the information provided and giving a comprehensive review of the corporate client's business, the customer service officer may:

- **Harmonize** the beginning of the business relationship
- **Refuse** to do business
- **Refer** the matter to the MLRO for a final decision if the customer service officer is in doubt about how to proceed further. MLRO may approve / reject a corporate client's application.

5. CLIENT DUE DILIGENCE

The legal audit of clients during the intake procedure is a 3-4 step process customized to meet the legal requirements. The Customer Service Officer / Compliance Officer identifies the customer by obtaining various information during this process, which is then verified by the MLRO based on documents, data and other information obtained from reliable and independent sources.

5.1. SIMPLIFIED LEGAL AUDIT

In cases stipulated by applicable law, the Company may apply a simplified legal audit.

In applying the simplified legal audit, the Company continues to monitor business relationships on an ongoing basis.

5.2. PRE-SELECTION OF CORPORATE CLIENTS

Regardless of the type of business and level of risk (except in the case of a simplified legal audit), the Company agrees that all potential corporate clients should be provided with a basic standard set of data including:

- A completed request and questionnaire (Attachment 3), which includes information about the client and the Beneficial Owner(s), as well as information about the purpose, intended nature and details of the activity.

- ID (a scanned copy of a photo ID of the Legal Representatives and/or Trustees and Beneficial Owners).

- Proof of address (scanned copy of the last 3 months utility bill of the Legal Representatives and/or Trustees and Beneficial Owners).

The Customer Service Officer checks that all fields of the Questionnaire have been completed, the information is clear, not contradictory and provides insight into the Corporate Client, Beneficial Owners and business activities.

In the event that the application form and/or ID and proof of address cannot be accepted for any reason (e.g. the photo ID does not look authentic, the application form provides contradictory information, etc.), the customer service officer has the right to reject the application.

In the event that the customer service officer agrees both the questionnaire and the ID and proof of address, then, based on the information,
received in the questionnaire, the Compliance Department will also perform the following checks:

- Verification of clients/Beneficial Owners against the RER lists/form; (Annexure 6).

- Verification of the client/Beneficial Owner/legal representatives against any of the sanctions lists below:
- List of United Nations counter-terrorism regulations published and tested in Canada pursuant to United Nations Resolution.

FINANCIAL SANCTIONS CHECK

- Sanctions of the Office of Foreign Assets Control of the Ministry of Finance Treasury Department U.S. (http://sdnsearch.ofac.treas.gov/Default.aspx)

COUNTRY CHECK

- List of risk countries according to the Financial Action Task Force (FATF) (http://www.fatf-gafi.org/topics/high- riskandnon- cooperativejurisdictions/)

The Company's system checks whether a number of parameters submitted by the applicant meet the criteria set out in the Company's blacklist. These criteria are as follows:

- The country of application/country of incorporation is not a country from which the Company is prohibited from operating. These countries will always include all countries and territories that do not cooperate with the FATF(NCCT) and will additionally include any country that is deemed (based on an internal risk management process) to pose too high a risk to do business with its residents;
- Names of known or suspected fraudsters / money launderers / terrorists. This criterion includes the names of customers who have defrauded or attempted to defraud the Company and those people who have been blacklisted by a published public notice;
- Check whether the country of registration is on the list of high-risk countries;
- Collect publicly available information (Internet) about the corporate client / Beneficial Owner / legal representatives to ensure that the corporate client / Beneficial Owner / legal representative is not a criminal,
- No suspicion of money laundering or terrorist financing or any attempt at such activity;
- Verify that the geographic areas of operation are not on a list of prohibited countries and that this does not constitute a legal impediment (government sanctions) to providing them with the requested Services.
- Confirmation that the corporate client's company name is not associated with any online complaints.

If the compliance department has determined that the potential client's country of jurisdiction and/or the risk associated with the geographic areas of operation are the same as those listed, further review will be required by forwarding the information to the MLRO,

If sanctions against a particular country include restrictions on cooperation with that country, MLRO:

- Decides not to initiate a Business Relationship with a potential Corporate Client;
- Informs a specific customer service officer of the inability to establish a business relationship with a corporate customer;
- Informs FINTRAC of its decision.

If the potential client has not provided the completed Questionnaire and the required information, the Company does not process the application,

The Company reserves the right not to send the report to FINTRAC, as at this stage of establishing a business relationship with a potential client, the Company cannot be sure that the reluctance of a potential corporate client is related to the compliance with the requirements (standards) of the legislation, and is not related to unwillingness to cooperate with the Company.

5.3. PRIVATE INDIVIDUAL PRE-SELECTION

The Customer Service Officer checks that all fields of the Questionnaire have been completed, the information is clear, not contradictory and provides insight into the Corporate Client, Beneficial Owners and business activities.

In the event that the application form and/or ID and proof of address cannot be accepted for any reason (e.g. the photo ID does not look authentic, the application form provides contradictory information, etc.), the customer service officer has the right to reject the application.

In the event that the customer service officer reconciles both the questionnaire and the identity and address verification, then, based on the information obtained on the questionnaire, the compliance department will also perform similar checks.

5.4. DOCUMENTATION REQUIREMENTS

The following basic documents are required for "Individuals":

- fully completed section of the CPS (customer due diligence) (Annex 2)
- National identity document
- Utility bill
- Summary
- Tax return
- Fully completed KYC section (Appendix 2)

In case of "corporate clients", after verifying the documents and information, the customer service officer should request:

- A scanned copy of the corporate client's articles of incorporation and/or constituent documents and certificate of incorporation;
- If the legal entity has been registered for more than one year (or depending on the country of incorporation of the corporate client - 1.5 years ago), a scanned document confirming its active status (e.g. certificate of proper registration and operation of the legal entity);
- A scanned copy of the Notice of Authorization to Sign, Power of Attorney or other document confirming the authority of the Legal Representative and/or authorized person.
- A scanned document confirming the status of the Beneficial Owner (e.g. Share Certificate, Declaration of Trust, Trust Deed).
- Documentation may be e-mailed for review by a customer service representative and records maintained. All relevant corporate customer information is updated and relevant documents are stored electronically in unique folders located on the Company's server. Hard copies of all key documents are kept at the Company's office.

The customer service officer will ensure that each scanned image received is stamped to indicate that the original has been certified by a competent authority.

Copies of documents received may be certified:

- By the Bank
- Notary
- Competent governmental or by a competent state or municipal registrar.

The submitted documentation must be of high quality and legible. The Company accepts

translations of documentation into languages understood by Company employees.

During the document review, the Customer Service Officer/Regulatory Compliance Officer certifies that:

- The document is valid;
- There are no clear signs tampering (strange smudges, damage to the document, etc.);
- The quality of the documentation (in terms of content, quality, possible errors) complies with the legislation.

Once the customer service worker has received the documentation, he/she should enter all pertinent information that should be included in the customer's case/file into the database.

The customer service officer should delay initiating a business relationship with the by a corporate customer prior to MLRO approval/denial if:

- The Customer Service Officer has reasonable doubts about the veracity of the information provided by the customer and/or has doubts about the Beneficial Owner (e.g. professional experience regarding date of birth), and/or the Customer Service Officer has found any compliance with the List of Suspicious Indicators (Annex 2) and the Customer Service Officer is unable to verify or confirm the information;
- It is established that the client / Beneficial Owner / legal representative is a politically exposed person and/or it is established that the client / Beneficial Owner / legal representative has a criminal record for or is involved in money laundering or terrorist financing, or in any of the following attempted such activities or are subject to criminal prosecution;
- The country of incorporation of the corporate client is included in the list of high-risk jurisdictions.

5.5. CONFORMITY ASSESSMENT

Once the legal documents are received, it is necessary to determine the suitability of the corporate client with the information received for the purpose of customer due diligence (KYC).

The Compliance Department will utilize the following metrics, which are ultimately related to:

Corporate client activities

A risk score is assigned depending on the type of product/service offered
Corporate Client, in accordance with the list of activities established by the Company (Appendix No. 3). The included activities are classified according to low, medium or high risk.

Country risk of a corporate client

Country of any potential corporate client (including directors and BSs) is checked against the list of high-risk countries and the Financial Action Task Force.
Risk Description:

- Blocked

"Prohibited" FATF countries and those countries with which the Company does not wish to do business for legal reasons,

- High

Countries that are considered to be at high risk of financial crime and where there is no immediate or effective automated KYC solution.

- Medium

Countries where there is a risk of financial crime and there is no immediate
KYC automated solution.

- Low

Politically and economically stable countries with relatively low risk of financial crime and with effective automated or manual electronic KYC solution

The Company will not offer products or services to corporate customers residing in "blocked" countries.

Corporate client legal form risk

In cases where a potential corporate client has a different type of legal form / corporate structure, the regulatory affairs department may contact the MLRO to find out what specific information needs to be collected and verified.

LOW RISK

- An entity listed on a regulated market (within the meaning of PCMLTFA and FINTRAC rules) of an international market that is subject to certain disclosure obligations;
- A consolidated subsidiary with a controlling interest in such a quoted company;
- Organizations whose structure and form of ownership are clear and understandable;
- Organizations are well-known, respected organizations with a long history in their industry and extensive public information about them;
- Canadian government agencies
- A private organization that is associated with an existing trusted corporate client or has a bank account with a registered bank.

MEDIUM RISK

- A legal entity whose composition of owners or participants makes it difficult to establish the Beneficial Owner, but the organization has a bank account with a registered bank;
- societies.

HIGH RISK

- Organizations with capital in the form of bearer shares;
- Non-governmental, supranational и State organizations;
- Philanthropy;
- Trusts and Foundations;

Private individual risk

The risk assessment can be affected if a RER has been identified on the board of the corporate or personal client that submitted the application. Once a risk assessment has been assigned, the compliance department must complete the client information to be included in the corporate client's case/file.

5.6. FINAL DECISION

Based on the risk assessment performed Corporate clients can be categorized into clients with:

- Low risk
- Medium risk
- High risk LOW RISK CLIENTS

If a corporate customer is classified as a "low risk" customer, the compliance department will review publicly available information about the corporate customer and, if so, seek MLRO and Board approval before initiating any business relationship. If negative, the compliance department will refer the application to the MLRO for review.

MEDIUM/HIGH RISK CUSTOMERS

If a corporate client is classified as a "medium or high risk client", then the compliance department will need to refer the application to the MLRO, who will conduct further due diligence before deciding whether to reject the application or sign it. When conducting further due diligence, the MLRO may request:

At a medium-risk corporate client: resume and additional documentation (e.g., copy of educational diploma) of the Beneficial Owners;

For a high-risk corporate client: resume or publicly available information, copy(s) of education diploma or documents confirming ownership of real estate or movable property, and/or documents confirming solvency, or a letter of recommendation for Beneficial Owners.

By analyzing the business or personal activities of the corporate client and ascertaining the origin of the corporate client's financial sources, the MLRO assesses the need to visit the corporate client's location to confirm that the information about the Beneficial Owner and business activities provided by the corporate client is true.

If the MLRO, after conducting a legal audit, feels that there is a need to visit a corporate client, he/she will inform the Customer Service Officer who serves the corporate client concerned.

After the visit, the customer service officer:

- Prepares a written (electronic) report in which he/she records the information obtained;
- Provides this report to the MLRO;
- Records / enters new information (if any) into the corporate client file.

If approved by the MLRO, the Customer Service Officer must obtain final approval from the Board before initiating any Business Relationship with a corporate customer.

6. LEGAL DUE DILIGENCE OF EXISTING CLIENTS

With respect to all Clients, the Company ensures that Business Relationships are continuously monitored to identify any suspicious activity, As legal due diligence is an ongoing process, the Company takes measures to ensure that Client profiles are up to date,

The Company uses the following measures to ensure that information about the Client is up-to-date, accurate and complete:

- Monthly AML check.

Any existing client (including legal representatives and Beneficial Owner) is automatically screened against the Financial Sanctions List and OFAC SDN List.

- Annual account verification and AML verification.

A full AMG audit, similar to the registration process, is conducted by the Compliance Department. When conducting a legal audit of a Client, the Company considers information already contained in their files that may confirm the identity of the Client or publicly available information to confirm information held by the Company. Any changes to the Client's information are updated in the database and the relevant documents are stored electronically in the Client's unique folder and in hard copy format at the Company's office.

7. EXTENSIVE DUE DILIGENCE

In the course of a business relationship, the MLRO determines the need for an enhanced legal audit when:

- A request has been received from FINTARC, pre-trial investigation authorities, prosecutor's office or court that is related to AML/CFT or other criminal activity;
- Information obtained from third-party / publicly available sources shows that the Client or one hundred Beneficial Owner is a PEP and/or the Client/Beneficial Owner or Legal Representative has a criminal record or is involved in money laundering or terrorist financing, or any attempt at such activities;
- When monitoring, suspicions arise that Customer transactions, or the volume of transactions, or the volume of Customer transactions, are associated with AML/CFT;
- The customer accepted an unusually large transaction with no apparent economic or legitimate purpose.

If any of the Customer's transactions meet the specified criteria, MLRO will verify the Customer's file(s) and the included information (if there are any updates) by performing the following steps:

- Compares the match between the Customer's completed transactions and reported personal/business activity;
- Verifies that the Beneficial Owner indicated by the Client or clarified by the Company is the true Beneficial Owner of the Client;
- Finds out the origin of the Client's financial resources and analyzes the Client's personal/business activities.

8. CUSTOMER MONITORING

The company divides customer monitoring into two types:

- Regular authorization and transaction verification performed by the MLRO department, whose responsibilities include:
- Monitoring the payment processing system to detect and prevent fraud,
- Entering transactions into the system and collaborating with Customer on transactions;
- Configure risk management system settings for client transactions to prevent fraud risk;
- Organization of interaction with Customers to investigate payment fraud and take measures to prevent recurrence of incidents.
- Implementation of AML prevention rules by the compliance department The compliance department is responsible for assessing the need for enhanced legal auditing and obtaining relevant documentation from the Client in the course of the business relationship.

8.1. REAL-TIME CUSTOMER MONITORING

The Company uses the System to analyze and track transactions made in the course of business relationships. A monitoring system is built into the system to flag transactions for further investigation. Monitoring is done in real time, generating automated reports for the IT department. These reports are reviewed by the IT department on an ongoing basis MLRO decides whether further assessment is required and assigns responsibility and timeframes for these reviews before taking appropriate action, if any.

Unusual transactions/actions that are detected automatically include:

- Transactions that differ significantly from the customer profile compared to the historical average, size, frequency, volume, origin, etc.
- Transactions in a Customer's dormant account or in an inactive relationship (e.g., Customers who have not been in contact with the Company for some time).

Regardless of the Customer's risk level, IT implements fraud prevention measures on a daily basis by performing the following Customer oversight activities:

- Daily fraud investigations.
- Weekly fraud investigation.
- Monthly fraud investigations.

If IT identifies any violations and/or non-compliance and

/ or rapid fluctuations in performance and/or exceeding the metrics specified in the vendor information, then the IT department will immediately sends an electronic request to the Customer Service Officer, who immediately sends an electronic request to the Customer with a list of the necessary documentation that must be provided to determine the cause of the discrepancy.

After evaluating the information received, the Customer Service Officer sends the Customer information / other information obtained during monitoring to the MLRO / Compliance Department, which makes a decision on further cooperation with the Customer.

If the Customer's violations involve risks unacceptable to the Company, MLRO has the right to suspend the Customer's transactions.

If MLRO after evaluating the information / documentation provided by the Customer and the Customer Service Officer decides to terminate the Business Relationship with a particular Customer, then:

- no later than ten (10) business days in advance, it shall include information about a particular Customer in the List of Rejected Customers;
- prepares and sends a report to FINTRAC;
- informs both the Compliance Department and the Customer Service Officer of its decision.

8.2. AD HOC AND POST-EVENT MONITORING (MLRO)

MLRO will also implement a number of ad hoc (e.g., randomly selecting a Customer and conducting additional due diligence, etc.) and post-event controls to strengthen the level of control and to ensure that Company personnel are following procedures.

- Identifying unusual / suspicious activity

The list of indicators of suspicious transactions was formed taking into account the best international practices. The Company may consider some transactions as suspicious based on their subjective assessment.

Suspicion means subjective perception (attitude) of the Company's personnel to the transaction made by the Client, which is manifested as distrust to a particular event or fact. The reason for distrust is the difference between the presented situation and the general / real situation and the real situation understandable for the Company's employees.

Company personnel are not liable for erroneous suspicion unless done with malicious intent.

Company personnel may not inform the Client or a third party of the existence of an internal report,

The Customer Service Officer is responsible for monitoring unusual activity independently and should flag it and report it to the MLRO for Level 2 review before taking any action.

Unusual transactions / actions, that must manually detect by the customer service officer include:

- Request for change of current account;
- Any changes in Customers' activities without prior notice.
- Identifying suspicious transactions:
- Receiving information from Company employees;
- Analyzing the Company's account statements, verifying that the Client's transactions are typical and consistent with the Client's business activities;
- Receiving information from FINTRAC on persons / companies / countries with whom the Company has a high risk of involvement in AML/CFT;
- By verifying the engaged Client's data and its compliance.

9. SUSPICIOUS ACTIVITY REPORTING

9.1. SUSPICIOUS ACTIVITY DETECTION

Every employee of the Company must report on information they receive in the course of their daily duties, namely when they know, suspect or have reasonable grounds to know or suspect. that a Client is engaging in or attempting to engage in money laundering or terrorist financing.

9.2. INTRODUCTION

Company personnel must report to MLRO any knowledge or suspicion of money laundering or terrorist financing.

Every employee of the Company must report to the MLRO if he/she has reason to know or suspect that a Customer is involved in or is attempting to engage in money laundering or terrorist financing.

Any Company employee who fails to fulfill these obligations without good cause may be subject to disciplinary and/or criminal penalties.

These procedures cover two main areas:

- Internal reporting - suspicious activity is identified by an employee who reports to the MLRO;
- External Reporting - when the MLRO reviews an internal report and decides whether to send the report to PCMLTFA and FINTRAC

All suspicions reported to the MLRO should be documented or recorded electronically. Reports should include client details and a full explanation of what information led to the initial suspicion.

All employees should be aware that once disclosed to MLRO or FINTRAC, it is a criminal offense to disclose any information that may "tip off" any interested party that a proceeding has been initiated against them, or to engage in any other activity that may prejudice an investigation.

Once the Company's employees have properly reported suspicions to the MLRO, the MLRO will proceed to assess the report received.

MLRO:

- Reviews each of the reports received;
- Defines, whether whether a specific report grounds for knowledge or suspicion.

To fulfill its mission, the MLRO has access to any information, including CUS information, in the possession of the Company that may be relevant. The MLRO has full access to all information available in the database. This includes all information collected during Client registration as well as all transactional information within the Business Relationship, All reports, as well as internal inquiries made regarding the report, are electronically logged and stored in a dedicated folder on the Company's server.

MLRO may also require additional information from the Customer.

The above information shall be obtained from the Client by the specialist for

customer service.

After gathering all the information, the MLRO decides whether to report to PCMLTFA and FINTRAC.

After evaluating and analyzing all available information, if the MLRO determines that the report provides grounds for certainty or suspicion, he/she will notify FINTRAC of a suspicious Customer transaction if:

- Identified transactions do not have rational purpose and do not correspond to the Client's personal/business activity;
- Transactions do not correspond to the types and volumes of transactions typical for the Client;
- If the requested documents are not received from the Customer or they do not eliminate suspicions.

MLRO does not prepare a report to FINTRAC if the information/documentation provided by the Client and the information obtained from the Client's enhanced legal audit eliminates suspicions of AML/CFT

- EXTERNAL REPORTING

Any MLRO reports to PCMLTFA and FINTRAC are run through a system pre-defined by FINTRAC.

MLRO reports to FINTRAC any transaction or activity that, after its assessment, it suspects or has reasonable grounds to allege or suspect links to money laundering or terrorist financing, or attempted money laundering or terrorist financing.

A report to FINTRAC is made as soon as possible after the information is received by the MLRO and the MLRO determines that such a report is due.

The following key information is included in the MLRO report:

- customer identification data;
- Details of the transaction or activity;
- Full details of why the MLRO suspects that a transaction or activity may be linked to money laundering or terrorist financing;
- The date on which the suspicious transaction or action occurred.
- Other information (if applicable).

If the MLRO chooses not to notify FINTRAC, the reasons for doing so must be clearly documented or electronically recorded and retained in an internal suspicion report.

MLRO maintains records of reports submitted to FINTRAC electronically.

All records shall be kept secure and confidential by MLRO for a minimum of five (5) years.

10. DECISION ON REFUSAL TO EXECUTE THE TRANSACTION

The Company has the right to refrain from executing transactions that are subject to additional verification due to information received by the Company that indicates that the transaction is illegal and/or abusive activity of the Client, if AML/CTF information is available.

The Company may not execute any Client transaction if the MLRO has chosen to refrain from executing one or more transactions or debit transactions of a particular type within a 31-day period and has reported this to FINTRAC.

If FINTRAC has issued an order to suspend one or more transactions or debit transactions of a particular type, the Company shall continue to refrain from executing one or more transactions or debit transactions of a particular type during a specified time period and the MLRO prepares a letter to that effect.

11. CUSTOMER TERMINATION

If the Client fails/refuses to provide the requested information and documentation that would allow the Company to conduct a substantive review, or the provided documentation does not eliminate suspicions regarding AML/CTF. The business relationship with the Client shall be terminated at the Company's initiative.

The Agreement may be terminated at the Company's initiative by informing the Client electronically/written if the Company has determined that:

- Client provided information o about himself, which misleading misleading / untrue;
- The Client fails to comply with the Agreement;
- The Client is involved in actions that are detrimental to the Company's image;
- The Client is affiliated with AML/CTF, or there is reasonable suspicion of the Client's affiliation with AML/CTF;
- The client is recognized as insolvent;
- The Client has not informed the Company of any changes in its beneficial ownership, shareholder structure or shareholdings;
- The volume and/or amount of the transaction is different from the transaction profile;
- The Client has changed the type of business activity without the written consent of the Company.

12. ACCOUNTING

The Company has established an appropriate accounting procedure to fulfill the Company's obligations with respect to the prevention of money laundering and terrorist financing.

Upon termination of the Business Relationship with the Client, the Client's file shall be retained for at least 5 years.
All information/documentation obtained during Client monitoring, as well as certified copies of identification documents, Beneficial Owner certificates, Client Questionnaire, other documentation obtained during the initial due diligence shall be kept in the Client file.

The Company's records include:

- Customer Information;
- Transactions;
- Internal and external suspicion reports;
- MTCO annual (and other) reports;
- Training and compliance monitoring;
- Information on the effectiveness of the training.

- The Company's accounting procedures:

- **Customer Information**. The Company shall retain information recorded electronically and stored in a customer folder maintained by the Company's server. Hard copies of relevant documentation shall be retained by the MLRO at the Company's office.

- **Transactions**. The Company is required to keep information about all transactions in the course of the business relationship.
All transaction records are stored in the transaction database.

- Internal and external suspicion reports, MLRO annual (and other) reports.

- The company must keep information related to MLRO (records of actions taken in accordance with the requirements of internal and external reporting; a record of information or documentation when the MLRO has reviewed any information or other documentation relating to possible money laundering but has not submitted a report to the PCMLTFA and FINTRAC; and copies of any reports submitted to FINTRAC and MLRO reports to the Board) both electronically in a dedicated MLRO reports folder on the Company's server and in hard copy format.

- Training (training effectiveness including). The Company shall store anti-money laundering training information electronically in a dedicated training folder on the Company's server, including:

- Training dates;
- Nature of learning
- Information on employees who have undergone training
- Employee testing results.

The Company shall retain any information that is required to be retained in accordance with this AML Policy:

- in the form of original documents:
- in the form of photocopies of original documents;
- in scanned form;
- electronically.

Records of ongoing investigations must be retained by the Company until the appropriate law enforcement authorities confirm that the case has been closed. If the Company has not been notified of an ongoing investigation within five years of the disclosure, the records must be destroyed.

13. TRAINING

The company will provide necessary training, procedures The Company will provide the necessary training, procedures and materials to familiarize employees with their responsibilities and enable them to comply with the AML policy. However, it is the personal responsibility of all employees to ensure that they are aware of and comply with this AML policy and related procedures.

Personnel training is carried out regularly, at least once a year, as well as in cases of changes in internal/external regulations related to money laundering or terrorist financing.

As the MLRO is responsible for overseeing the Company's anti-money laundering systems and controls, it is also responsible for ensuring that the Company's employees

are adequately trained in relation to anti-money laundering.

The Company ensures that staff are aware of the money laundering / terrorist financing risks and are well trained to identify unusual activities or transactions that may be suspicious.

The Company acts appropriately to ensure that:

- all relevant employees are familiarized with the rules relating to money laundering and terrorist financing;

- all relevant employees are regularly trained to recognize and deal with transactions that may be related to money laundering or terrorist financing.

The company ensures that employees are knowledgeable:

- Their responsibilities in accordance with the Company's arrangements for the prevention of money laundering and terrorist financing;

- Identities and responsibilities of the MGCO;

- The Company's legal and regulatory obligations in the area of money laundering / terrorist financing risk management.

The MLRO keeps a log to keep track of. who has been trained, when the training took place, the nature of the training provided and its effectiveness. All employees must sign the training log to confirm that they have received training.

13.1. NEW EMPLOYEES

New employees are trained within four weeks of joining the Company. All new employees of the Company receive general training on AML-related issues, which includes:

- Regulatory environment and implications for the Company;
- AML/CFT risks relevant to the Company;
- MLRO Identities and Responsibilities;
- Internal policies and procedures in place;
- Measures of legal audit monitoring/extended legal audit of the client;
- Suspicious Activity - how to recognize unusual or suspicious transactions, indicators of reasonable grounds to allege or suspect that money laundering or terrorist financing is taking place;
- How to send an internal MLRO report;
- Recordkeeping Requirements.

The information presentation and all anti-money laundering documentation will be available to all employees throughout their employment with the Company.

13.2. TRAINING AND AWARENESS REGARDING AML/CFT FOR CUSTOMER SERVICE OFFICER / REGULATORY AFFAIRS DEPARTMENT LEGAL COMPLIANCE

The Customer Service Officer and the Compliance Department are trained regularly, at least once a year, as well as in cases where amendments / changes have been made to internal / external regulations related to money laundering or terrorist financing.

MLRO educates employees on how their products and services can be used as a means of money laundering or terrorist financing and informs them about:

- Importances KYC, including identification Customer, obtaining

additional information and monitoring the Client's activity;

- The Company's policies and procedures regarding the prevention of money laundering and terrorist financing
- Anti-Money Laundering Regulations;
- Criminal law, relating to laundering money and terrorist financing;
- FINTRAC requirements;
- Risks, associated money laundering and terrorism financing for the Company's products and services.