HONOR GLOBAL MARKETS LIMITED

Anti-Money Laundering Compliance Program

in accordance with
Proceeds of Crime (Money Laundering) and Terrorist Financing Act

Version: October 2023

Table of Contents

Paragraph 1: Background and Overview

Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA") came into operation in 2000, with latest amendments in June 2023. Under the PCMLTFA, all Reporting Entities ("RE") are required to comply with the PCMLTFA.

As HONOR GLOBAL MARKETS LIMITED ("Company") is a licensed Money Services Business ("MSB") in Canada, it is currently subject to the PCMLTFA and is regulated under Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). The Company is aware of the risk of potential Money Laundering and Terrorist Financing ("ML/TF") activities that could take place via the platform and solutions it offers. The Company is therefore committed to maintaining and executing AML/CFT controls to address concerns around the robustness of its controls to detect and deter ML/TF risks and manage the risks to which it may be exposed.

Also, it is the responsibility of each financial institution to put in place its own policies, procedures and controls to mitigate the risks of ML/TF. In this regard, the Company has this AML Compliance Program ("Compliance Program") and AML compliance policies and procedures ("compliance policies and procedures") in place.
Ref: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng

Company Profile

Company Name:	Honor Global Markets Limited
Corporation Number:	1160432-5
Date of incorporation:	04 September 2019
Shareholder:	Future Honor Limited (100%)
Directors:	CAI Ming
Address:	250 Yonge Street, Suite 2201, Toronto, ON, CA M5B2L7, Canada
Company Structure:	Limited company incorporated in Canada
Nature of Business:	Money Service Business
Client Identity Verification:	Yes, and procedures are in place in accordance with the laws of Canada
Client Identity Verification:	Yes, and procedures are in place in accordance with the laws of Canada
Compliance Officer:	Jim Chan

About the Company

The Company was incorporated in Canada on 4 September 2019. The Company is the money service arm of the Future Honor Group (www.futurebank.global) in Canada. The Group's mission is to empower our clients with seamless cross-border transactions and global banking solutions, paving the way for a connected, prosperous future.

Compliance Program

This Compliance Program is intended for all staff relating to the day-to-day operation of HONOR GLOBAL MARKETS LIMITED ("the Company"). It sets out the responsibilities and obligations of Senior Management, Compliance Officer ("CO") and staff, together with the Company's standard operating and compliance procedures under PCMLTFA.

This Compliance Program is established and implemented by the Company and is intended to ensure its compliance under the PCMLTFA and associated Regulations. The Compliance Program forms the basis for meeting all of the reporting, record keeping, client identity verification and other Know-Your-Client requirements under the PCMLTFA and associated Regulations. The purpose of this Compliance Program is to raise awareness, ensure proper compliance with the laws and regulations, promptly address irregularities and create a better practice environment in the Company.

Under the PCMLTFA, the Company, as an RE, is required to:

(a) Appointing a Compliance Officer who is responsible for implementing the program;

(b) Developing and applying written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer;

(c) Conducting a risk assessment of the Company's business to assess and document the risk of a money laundering offence or a terrorist activity financing offence (ML/TF) occurring in the course of the Company's activities;
(d) Developing and maintaining a written, ongoing compliance training program for the Company's employees, agents or mandataries, or other authorized persons;
(e) Instituting and documenting a plan for the ongoing compliance training program and delivering the training (training plan); and
(f) Instituting and documenting a plan for a review of the compliance program for the purpose of testing its effectiveness and carrying out this review every two years at a minimum (two-year effectiveness review).

The Company's compliance policies and procedures must be:
(a) Written and should be in a form/format that is accessible to its intended audience;
(b) Kept up to date (including changes to legislation or the Company's internal processes, as well as any other changes that would require an update); and
(c) Approved by a senior officer, if the Company is an entity.

The policies and procedures should be made available to all those authorized to act on the Company's behalf, including employees, agents and any others that deal with clients, transactions, or other activities.

The Company's compliance policies and procedures should cover the following requirements as applicable to the Company as an RE:
(a) Compliance program requirements: this includes the Company's requirements to have an appointed compliance officer, a risk assessment, an ongoing compliance training program and plan, and a two-year effectiveness review and plan, which consists of a review of the Company's policies and procedures, risk assessment, and ongoing training program and plan;
(b) Know Your Client requirements: this includes the Company's requirements for verifying client identity, politically exposed persons, heads of international organizations, their family members and close associates, beneficial ownership, and third party determination;
(c) Business relationship and ongoing monitoring requirements;
(d) Record keeping requirements;
(e) Reporting requirements;
(f) Travel rule requirements: this includes the Company's requirement to develop and apply written risk-based policies and procedures to help determine whether it should suspend or reject an electronic funds transfer ("EFT") or Virtual Currency ("VC") transfer that it receives, and any other follow-up measures, if the transfer does not include the required travel rule information and the Company is unable to obtain this information through the Company's reasonable measures; and
(g) Ministerial directive requirements.

Paragraph 2: AML Framework and Objectives

The Company takes all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF and to prevent a contravention of any requirement under the PCMLTFA.

The Company adopts a risk-based approach ("RBA") in the design and implementation of the Anti-Money Laundering ("AML") and Counter-Terrorist Financing ("CFT") policies, procedures and controls ("AML/CFT Systems") with a view to managing and mitigating ML/TF risks.

The Company is dedicated to defend and maintain the high-quality financial system of Canada through the implementation of effective AML/CFT policies, procedures and controls.

The Company establishes and implements adequate and appropriate AML/CFT Systems taking into account factors including types of clients, products and services offered, delivery channels and geographical locations involved.

Introduction of PCMLTFA

What is Money Laundering and Financing of Terrorist?

Money Laundering ("ML")

According to the FINTRAC, "Money laundering" ("ML") is the process used to disguise the source of money or assets derived from criminal activity. There are three recognized stages in the money laundering process:

(a) Placement involves placing the proceeds of crime in the financial system.
(b) Layering involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
(c) Integration involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The money laundering process is continuous, with new 'dirty' money constantly being introduced into the financial system.

In any event, no matter what the criminal may do, the criminal may want to achieve three things:

(i) Conceal the true ownership of the money and where it came from;
(ii) Keep control of the money, and
(iii) Change its form.

Terrorist Financing ("TF")

According to the FINTRAC, Terrorist activity financing ("TF") is the use of funds, property or other services to encourage, plan, assist or engage in acts of terrorism, where the primary motivation is not financial gain.

Two main differences distinguish terrorist activity financing from money laundering:
(a) Funds can be from legitimate sources, not just criminal acts; and
(b) Money is the means, not the end—the goal is to use funds to facilitate or implement terrorist activities.

Terrorist Financing generally covers the carrying out of any transaction that involve funds owned by terrorists, or that have been, or are intended to be, used to facilitate the commission of terrorist acts.

Similar to money laundering, terrorist financing also aims at disguising the origins of funds, but its focus is on the directing of fund, whether legitimate or not, to terrorists. In terrorist financing, the key fact is on the destination or use of funds, which may have been derived from legitimate sources.

Typical signs or indicators for ML/TF

The Company adopts the SAFE approach for identifying typical signs or indicators for ML/TF:
Screen: Screen the account for suspicious indicators: Recognition of a suspicious activity indicator or indicators.
Ask: Ask the client appropriate questions
Find: Find out the client's records: Review if information already known when deciding if the apparently suspicious activity is to be expected.
Evaluate: Evaluate all the above information: Is the transaction suspicious?

Typical red flags indicators include, but not limited to:
(a) Transactions involving amounts just below reporting thresholds (i.e., structuring)
(b) Split transfers or cash withdrawals into amounts just below cash transaction reporting thresholds.
(c) Fund withdrawals by legal representative without apparent business reason.
(d) Frequent and substantial wire transfers from/to high tax jurisdiction without a legitimate commercial purpose.
(e) Excessive withdrawals or deposits in which the origins are not justified or inconsistent with the purpose of the account, as documented in the client file.
(f) Deposit of funds into an account which are found to be under a nominee name.
(g) Insufficient explanations with respect to the source and purpose of receipts.
(h) Transaction not commensurate with the known client profile or structure.

The Company adopts a risk-based approach (RBA) in the design and implementation of the Compliance Program with a view to managing and mitigating ML/TF risks.

Ministerial Directives and Transaction Restrictions

Under Part 1.1 of the PCMLTFA, the Minister of Finance may:

(a) Issue Directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
(b) Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering and terrorist financing.

The Directive will be issued by the Minister of Finance. However, FINTRAC will inform reporting entities that a directive has been issued. Each directive will be added below and will include an outline of countermeasures that are limited to the same activities for which reporting entities already have obligations. The countermeasures will enhance or add to these obligations.

The Directives will specify the date they come into force and will remain in force until officially revoked, suspended or amended. The Directives will be reviewed at least every three years from the day they take effect.

The authority to recommend new regulations to restrict certain transactions is intended to be used in the most serious of cases. The Minister of Finance must consult the Minister of Foreign Affairs before recommending regulations to the Governor-in-Council. These regulations will be published in the Canada Gazette and will be prepared on a case-by-case basis.

The Company will fully comply with the Ministerial Directives and Transaction Restrictions issued to the Company and will fully cooperate with the relevant authorities.

Paragraph 3: Allocation of Responsibilities

Obligations of Senior Management

The Company's senior management undertakes its assessment of the risks the firm faces and how the ML/TF risks are to be managed and ensures all relevant staff are trained and made aware of the law and their obligations under it.

To ensure compliance, the senior management should ensure:

(a) Policies and procedures for the prevention of ML/TF – the Company should establish appropriate policies and procedures for the prevention of ML/TF and ensuring their effectiveness and fully comply to existing regulatory requirements; such policies and procedures should be communicated and applicable to all levels of staff within the Company and reviewed regularly for the purpose of ensuring its up-to-date and effectiveness;

(b) The four keys of AML - The policies and procedures should be designed to fulfill the following:
- Client Identity Verification;
- Record Keeping;
- Ongoing monitoring; and
- Reporting of Suspicious Transactions.

(c) Compliance Officer - the Company should appoint a Compliance Officer who should have sufficient seniority and experience to which staff are instructed to report suspected ML/TF transactions to him/her;

(j) Full cooperation with law enforcement agency;

(k) Staff training – Staff training should be provided to ensure that all staff are familiar with and maintain sufficient level of awareness of local regulations and requirements for the prevention of ML/TF through orientation and regular training;

(l) Proper implementation of policies and procedures - Internal review should be carried out at least every two years to ensure proper compliance of the Company's policies and procedures for the prevention of ML/TF. In addition, the Company may consider engaging a professional consulting firm to perform independent reviews on the effectiveness of the policies and procedures, implementation status by the staff, and the accuracy and completeness of the reports.

In particular, under the PCMLTFA, the Company is required to appoint a Compliance Officer who:

(a) Have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes;

(b) Have knowledge of the Company's business's functions and structure;

(c) Have knowledge of the Company's business sector's ML/TF risks and vulnerabilities as well as ML/TF

trends and typologies; and

(d) Understand the Company's business sector's requirements under the PCMLTFA and associated Regulations.

The Company appoints a Compliance Officer ("CO") (named: Mr. Jim Chan) to act as a focal point for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed.

The Company adopts appropriate measures to enable frontline staff to know their responsibilities, to judge whether a transaction is suspicious and to report suspicion to CO in a timely manner. All employees must comply with the company's compliance policy. All employees must be vigilant and not allow the company to be used as a conduit for money laundering, terrorist financing, or other criminal activity (collectively referred to as "financial crime").

Obligations of Compliance Officer

The primary responsibilities of a Compliance Officer include:

(a) developing and/or continuously reviewing the Company's AML/CFT Systems to ensure they remain up to date, meet current statutory and regulatory requirements and are effective in managing ML/TF risks arising from the Company's business;

(b) overseeing all aspects of the Company's AML/CFT Systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;

(c) communicating key AML/CFT issues with senior management, including, where appropriate, significant compliance deficiencies; and

(d) ensuring AML/CFT staff training is adequate, appropriate and effective.

A Compliance Officer will also be responsible for the following:

(a) recommend and implement new procedures relating both to ML/TF and Due Diligence from time to time (where necessary);

(b) investigate all reports of suspicious transactions reported to him by his staff;

(c) prepare and submit regular and suspicious transaction report to the FINTRAC;

(d) ensure all blacklists in the Company's database are up-to-date and if such blacklisted the Company or individual tries to deal with the Company, staff and the Compliance Officer will be notified immediately;

(e) disseminate information relating to CIV and suspicious transactions to the Company's staff as early as practicable;

(f) provide training and regular meetings to the Company staff regarding the above;

(g) ensure compliance by all staff members of all their obligations set out in this operation manual and hand out disciplinary action when necessary;

(h) set a transaction limit, this transaction limit is a reference indicator based upon expected transaction information provided by the Account Bearing Client on opening their account. Once a transaction limit has been set, the Compliance Officer shall notify all staff and in particular the Account Managers of the limit and enter the information into the Company's database. If this limit should be exceeded, the CO shall consider whether or not to authorise such transaction and where necessary visit the Account Bearing Client to determine if the increase is based on a prospering business;

(i) the Compliance Officer shall review each Account Bearing Client's transaction position to consider, based on the needs of their business, if their transaction limited need to be adjusted;

(j) on reviewing the Account Bearing Client's position, the Compliance Officer or such other sufficiently experienced officer appointed by the Compliance Officer shall, amongst other things, do the following:

  i. make annual visits to the client;
  ii. review and where necessary update all client information;
  iii. verify any changes of the officers of the client against publicly available information;
  iv. see if there is any increase or decrease in transaction amounts and whether there is a need to vary existing limits;
  v. see if there is any change in the Authorised Contact Person;
  vi. make monthly cross references against Blacklists, if there should be any inconsistency between the information provided by the Account Bearing Client is inconsistent with searches made by the Company and the Company will suspend that client's account;

(k) In addition to the above, the Compliance Officer may sample check to see if the Client's answers are consistent with search results through an onsite visit or telephone interview. Where necessary, the frequency of visits may be increased as the need may arise, for reasons such as, but without limitation to:

  i. change of controlling shareholders or nature of business;
  ii. occurrence of abnormal transactions;
  iii. new developments of laws or matters either in general or in relation to that client's business;
  iv. developments brought to the attention of the Compliance Officer that the client may be subject to potential litigation;
  v. change of authorised person; or
  vi. client's request.

(l) advise the Account Bearing Client of changes in:

  i. money laundering laws;
  ii. notify them where in-depth information on the changes and updates can be viewed;
  iii. let them know of the common forms of money laundering activities and how they are carried out;
  iv. provide resources and answers to frequently asked questions on money laundering and CIV policies;

v. the Company's position on money laundering and the Company's reporting obligations and advising them that they should be familiar with CIV rules.

(m) review of internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the FINTRAC;

(n) maintenance of all records related to such internal reviews; and

(o) provision of guidance on how to avoid "tipping off".

Obligations of the Front-line Staff

The primary responsibilities of front-line staff include:

a) Recording and collecting clients' information and documents in the process of client recognition;

b) Asking appropriate questions and clarifying suspicious circumstances;

c) Reporting suspicious activity during the client recognition process to Compliance officer actively;

d) Being vigilant when clients ask about information on remittance to a high-risk country; and

e) Cooperating with Compliance Officer.

In addition to the responsibilities of different positions, internal communication is central to ensuring overall compliance and efficient operation. An open, transparent, and efficient communication mechanism is key to ensuring every team and employee understands and follows the Compliance Program and procedures.

The Company's Internal Communication Strategy:

(a) Regular Briefings: All relevant departments will receive regular updates and briefings on the Compliance Program and procedures, ensuring everyone is informed of the latest information.

(b) Cross-departmental Meetings: The Company will regularly organize cross-departmental AML working meetings, encouraging departments to share experiences, make suggestions, and collaborate.

(c) Online Platform: The Company has an internal online platform containing all materials related to the AML/CTF systems, which employees can access at any time.

(d) Open Door Policy: The Company encourages employees to communicate directly with the compliance and risk control teams whenever they have questions or suggestions about the Compliance Program and procedures.

The Company will take measures to ensure compliance with the relevant regulations and legislation on Financing of Terrorist. The legal obligations of the Company and those of its staff should be well understood and adequate guidance and training should be provided for the latter.

Paragraph 4: Client Identity Verification, Travel Rule Requirements, Record Keeping and Ongoing Monitoring

Client Identity Verification

The Company recognizes the importance of relationships with third parties and partners for the company's success. To ensure the safety and compliance of cooperation, we have formulated the following strategies:

(a) Background Checks: For all new clients, the Company will conduct Client Identity Verification ("CIV") through background checks, including their financial health, business reputation, and past compliance records.

(b) Ongoing Assessment: After establishing a relationship with partners and third parties, the Company will periodically assess their risk status and compliance performance, updating our strategies as needed.

(c) Contractual Terms: All contracts with clients will contain explicit compliance clauses, requiring them to adhere to all relevant laws, regulations, and best practices.

The Company carries out CIV measures under the conditions as stated in the PCMLTFA and uses RBA to adopt appropriate controls and oversight and accordingly to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

The Company also reviews all clients that present high ML/TF risks annually or more frequently if deemed necessary to ensure the CIV information retained remains up-to-date and relevant.

The Company obtains the information on the purpose and intended nature of business relationship of the client. The Company keeps the documents obtained in the course of identifying and verifying the identity of the client and maintains the documents obtained in connection with the transactions for at least 5 years.

Name screening of client (including each partner, director, officer, and authorized signatory of an entity) and beneficial owner will be performed through various means, including a check against Dow Jones, the United Nations sanctions list and the Office of Foreign Assets Control sanctions lists. Such name screening will be conducted before client onboarding or processing transactions (including originator, recipient and beneficiary institution). Periodic name screening will be also conducted on the client base.

The Company will apply for an RBA when conducting CIV measures and the extent of CIV measures should be commensurate with the ML/TF risks associated with a business relationship. Where the ML/TF risks are high, the Company will conduct Enhanced measures.

The Company must verify the identity of clients for the following:

(a) Large cash transactions
(b) Large virtual currency (VC) transactions
(c) Suspicious transactions
(d) Issuing or redeeming traveller's cheques, money orders, or similar negotiable instruments of $3,000 or more
(e) Transmitting $1,000 or more in funds by means other than an electronic funds transfer (EFT)
(f) Initiating an EFT of $1,000 or more
(g) Foreign currency exchange transactions of $3,000 or more
(h) Transferring VC in an amount equivalent to $1,000 or more
(i) Exchanging VC in an amount equivalent to $1,000 or more
(j) Remitting funds in the amount of $1,000 or more to a beneficiary, by means other than an EFT
(k) Remitting funds to the beneficiary of an international EFT of $1,000 or more
(l) Remitting VC to a beneficiary in an amount equivalent to $1,000 or more
(m) Information records
(n) Crowdfunding platform donation

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/client/msb-eng

CIV requirements should apply when the Company enters into a business relationship with a client. A business relationship is a relationship established between the Company and a client to conduct financial transactions or provide services related to financial transactions. In particular, as an MSB, the Company is considered as entering into a business relationship with a client when:

(a) the second time it is required to verify their identity within a 5-year period; or
(b) when it enters into a service agreement with an entity to provide any of the following services:
    (i) foreign exchange dealing;
    (ii) remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network;
    (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity; or
    (iv) dealing in virtual currencies.

    Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/brr-eng

Enhanced measures are the additional controls and processes that the Company has put in place to manage and reduce the risks associated with the high-risk clients and business areas. As part of the Compliance Program, the Company must develop and apply written policies and procedures for the enhanced measures that the Company will take for any ML or TF risks it identifies as high.

Account Opening Application

All clients, collectively referred to as "**Clients with business relationship**" who transact on a regular basis, must open and maintain an account by completing **Account Opening Form**.

The Company will not open account or trade with the following clients or their connected parties:

(a) Politically Exposed Persons ("PEPs") as defined under PCMLTFA;

(b) suspected terrorists; and

(c) sanctioned entities.

The Company will also not maintain any anonymous accounts or accounts in fictitious names.

With the Client Identification and Verification ("ID&V") and Know Your Client ("KYC") principles, the Company's **Account Opening Form** requires the applicant to provide substantial amount of information (where applicable), designated information means, in respect of a financial transaction, an attempted financial transaction or an importation or exportation of currency or monetary instruments:

(a) the name of any person or entity that is involved in the transaction, attempted transaction, importation or exportation or of any person or entity acting on their behalf (or "third party");

(a.1) the date of birth, gender, country of residence and nature of the occupation or business of a person referred to in paragraph (a), any alias that they use or have used and the name and business address of their employer;

(a.2) the nature of the principal business of an entity referred to in paragraph (a), the entity's registration or incorporation number and the jurisdiction and country of issue of that number;

(a.3) the following information in respect of a person or entity referred to in paragraph (a):

(i) their address, telephone number and electronic mail address,

(ii) any identification number assigned to them by the Company,

(iii) the Uniform Resource Locator of their website, and

(iv) the type of document or other information used to identify or verify their identity, the jurisdiction and country of issue of the document and the number of the document or the number associated with the information;

(b) the name and address of the place of business where the transaction or attempted transaction occurred or the address of the customs office where the importation or exportation occurred, and the date the transaction, attempted transaction, importation or exportation occurred;

(b.1) the purpose of the transaction, attempted transaction, importation or exportation;

(c) in the case of an importation or exportation, the amount and type of currency or monetary instruments;

(c.1) in the case of a transaction or attempted transaction,

(i) the amount and type of currency, monetary instruments or virtual currency involved, or

(ii) if no currency, monetary instruments or virtual currency is involved, the value of the transaction or attempted transaction or the type and value of the funds or other remittances that are the subject of the transaction or attempted transaction;

(c.2) the rate of exchange used in relation to the transaction, attempted transaction, importation or exportation;

(d) in the case of a transaction or attempted transaction,

(i) the manner in which the transaction was conducted, or the attempted transaction was to be conducted,

(ii) any transaction number, account number, institution number, branch number or similar identifying number involved,

(iii) the date on which any account involved is opened or closed, as well as its status,

(iv) the posting date,

(v) any identification number assigned to a person or entity referred to in paragraph (a) as part of the transaction or attempted transaction, and

(vi) the bank identification code or business entity identifier of any person or entity referred to in paragraph (a) that is a member of the Society for Worldwide Interbank Financial Telecommunication;

(d.1) in the case of a transaction or attempted transaction involving virtual currency or an electronic funds transfer as defined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, transaction identifiers, including sending and receiving addresses, and any username of a person or entity referred to in paragraph (a);

(d.2) in the case of a transaction or attempted transaction, the source of funds or of virtual currency and other related information including the name of the person or entity that is the source of funds or virtual currency, as well as the person or entity's account number, policy number or identifying number associated with the funds or virtual currency;

(d.3) in the case of a transaction or attempted transaction that, in whole or in part, is conducted online, the type of device used to conduct the transaction or attempted transaction, as well as the date and time of the transaction or attempted transaction;

(d.4) in the case of a transaction, whether it was completed or not;

(d.5) in the case of an incomplete transaction or an attempted transaction, the reason it was not completed;

(e) the name, address, electronic mail address and telephone number of each partner, director or officer of an entity referred to in paragraph (a), and the address and telephone number of its principal place of business;

(f) any other similar identifying information that may be prescribed for the purposes of this section;

(g) the details of the criminal record of a person or entity referred to in paragraph (a) and any criminal charges laid against them that the Centre considers relevant in the circumstances;

(h) the relationships suspected by the Centre on reasonable grounds to exist between any persons or entities referred to in paragraph (a) and any other persons or entities;

(h.1) in the case of a transaction or attempted transaction involving an electronic funds transfer as defined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, any information in respect of the relationships that exist between any persons or entities connected in any way to the transaction or attempted transaction, including any person or entity that initiates or may benefit from it;

(i) the financial interest that a person or entity referred to in paragraph (a) has in the entity on whose behalf the transaction was made or attempted, or on whose behalf the importation or exportation was made;

(j) the name of the person or entity referred to in paragraph (a) suspected by the Centre on reasonable grounds to direct, either directly or indirectly, the transaction, attempted transaction, importation or exportation;

(k) the grounds on which a person or entity made a report about the transaction or attempted transaction and any action taken by the person or entity as a result of the suspicions that led them to make the report;

(l) the number and types of reports on which a disclosure is based;

(m) the number and categories of persons or entities that made those reports;

(n) indicators of a money laundering offence or a terrorist activity financing offence related to the transaction, attempted transaction, importation or exportation;

(o) information about the importation or exportation sent to the Centre under Part 2;

(p) if the transaction is carried out by means of an electronic funds transfer as defined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, information about the transaction that is contained in a report made and that is remittance information as defined by the Society for Worldwide Interbank Financial Telecommunication;

(q) information about the transaction, attempted transaction, importation or exportation, received by the Centre from an institution or agency under an agreement or arrangement, that constitutes the institutions or agency's reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or an offence that is substantially similar to either offence;

(r) if an entity referred to in paragraph (a) is a trust, the name, address, electronic mail address and telephone number of every trustee and every known beneficiary and settlor of the trust;

(s) the name, address, electronic mail address and telephone number of each person who owns or controls, directly or indirectly, 25% or more of an entity referred to in paragraph (a), other than a trust, unless the trust is widely held or publicly traded; and

(t) information respecting the ownership, control and structure of an entity referred to in paragraph (a).

If the Enhanced Measures are required, the Company will lower ownership / control identity checking threshold to 10%, obtain documentary evidence on (e) above, and / or requiring the first payment to be carried

out through an account in the client's name with a bank subject to similar CIV standards.

Third party determination requirements

The Company must take reasonable measures to determine whether a third party is involved when :
(a) report a large cash transaction or keep a large cash transaction record;
(b) report a large virtual currency transaction or keep a large virtual currency transaction record;
(c) keep a signature card or an account operating agreement; or
(d) keep an information record.

Reasonable measures for third party determination could include asking the client if they are acting on the instruction of another person or entity, or asking whether another person or entity will be instructing on the account.
Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/tpdr-eng

Politically Exposed Persons (PEPs)

PEPs are defined as:
(a) a politically exposed foreign person, a prescribed family member of a politically exposed foreign person, or a person who the person or entity knows or should reasonably know is closely associated, for personal or business reasons, with a politically exposed foreign person;
(b) a politically exposed domestic person, a prescribed family member of a politically exposed domestic person, or a person who the person or entity knows or should reasonably know is closely associated, for personal or business reasons, with a politically exposed domestic person; or
(c) the head of an international organization, a prescribed family member of the head of an international organization, or a person who the person or entity knows or should reasonably know is closely associated, for personal or business reasons, with the head of an international organization.

Head of an international organization means a person who, at a given time, holds — or has held within a prescribed period before that time — the office or position of head of
(a) an international organization that is established by the governments of states;
(b) an institution of an organization referred to in paragraph (a); or
(c) an international sports organization.

Politically exposed domestic person means a person who, at a given time, holds — or has held within a prescribed period before that time — one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions

referred to in paragraphs (b) and (k):
(a) Governor General, lieutenant governor or head of government;
(b) member of the Senate or House of Commons or member of the legislature of a province;
(c) deputy minister or equivalent rank;
(d) ambassador, or attaché or counsellor of an ambassador;
(e) military officer with a rank of general or above;
(f) president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
(g) head of a government agency;
(h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
(i) leader or president of a political party represented in a legislature;
(j) holder of any prescribed office or position; or
(k) mayor, reeve or other similar chief officer of a municipal or local government.

Politically exposed foreign person means a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:
(a) head of state or head of government;
(b) member of the executive council of government or member of a legislature;
(c) deputy minister or equivalent rank;
(d) ambassador, or attaché or counsellor of an ambassador;
(e) military officer with a rank of general or above;
(f) president of a state-owned company or a state-owned bank;
(g) head of a government agency;
(h) judge of a supreme court, constitutional court or other court of last resort;
(i) leader or president of a political party represented in a legislature; or
(j) holder of any prescribed office or position.
Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-eng

When the Company initiates an international EFT/VC in the amount of $100,000 or more at the request of a person and determine that the person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, and based on the Company's risk assessment, it considers there to be a high risk of an ML or TF offence being committed, it must perform the following within 30 days:
(a) take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth; and
(b) ensure that a member of senior management reviews the transaction.

When the Company receives for a beneficiary an international EFT or an amount of VC equivalent to $100,000 or more and determine that the beneficiary is a domestic PEP, HIO, or family member or close

associate of a domestic PEP or HIO, and based on the Company's risk assessment, it considers there to be a high risk of an ML or TF offence being committed, it must ensure that a member of senior management reviews the transaction

The Company must keep a record of:
(a) the office or position and the name of the organization or institution of the PEP or HIO;
(b) the date of the determination;
(c) the source of the funds or source of the VC used for the transaction, if known;
(d) the source of the person's wealth, if known;
(e) the name of the member of senior management who reviewed the transaction; and
(f) the date of that review.
Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-non-acct-eng

Business relationships with individuals holding important public positions as well as persons or companies clearly related to them, (i.e., family members, close associates, etc.) expose businesses to particularly significant reputation or legal risks. There should be Enhanced Measures in respect of such PEPs, such as the verification of origins and circumstances of the transaction.

Whilst it is acknowledged that the majority of transactions are performed on behalf of occasional clients, business should endeavour to screen such transactions for the involvement of PEPs, their relatives or close associates. Businesses are expected to be vigilant and, when in doubt gather sufficient information from a client, and check publicly available information to establish whether the client is a PEP.

The Company adopts a risk-based approach for identifying PEPs and focuses on persons from countries that have a higher prevalence of corruption (reference can be made to for example to publicly available information such as the Corruption Perceptions Index). The involvement of a PEP in a transaction may be a factor in determining whether or not to file a disclosure.

Currently the Company does not accept PEPs client account opening applications.

Name Screening

On receiving the requisite information, the Compliance Officer shall conduct searches through publicly available sources. The names will also be checked against the UNSCCL and OFAC sanctioned list.

In addition to the above, our Compliance Officer uses internationally recognized professional governance tools: such Dow Jones, for strengthening Company's ability in global regulatory intelligence, financial crime,

enhanced due diligence, compliance management, internal audit and risk management.

The Company shall ensure that all forms and transaction details are completely and correctly filled in.

The Company adopts a risk-based approach to adopt appropriate controls and oversight and accordingly to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

The Company should monitor the business relationship with clients:

(a) Ongoing CIV: reviewing from time-to-time documents, data and information relating to the client that have been obtained by the Company to ensure that they are up-to-date and relevant; and

(b) Transaction monitoring:

(i) conducting appropriate scrutiny of transactions carried out for the client to ensure that they are consistent with the Company's knowledge of the client, the client's business, risk profile and source of funds; and

(ii) identifying transactions that

(A) are complex, unusually large in amount or of an unusual pattern, and

(B) have no apparent economic or lawful purpose; and examining the background and purposes of those transactions and setting out the findings in writing.

The Company should keep the documents obtained in the course of identifying and verifying the identity of the client and maintain the documents obtained in connection with the transactions throughout the business relationship with the client and for a period of at least five years after the termination of business relationship.

The Compliance Officer shall be responsible for informing the Senior Management on a timely basis if the Compliance Officer suspects a client involves in any money laundering or terrorist financing activities, or with any high-risk indicators identified. The Senior Management shall determine if have the authority to accept / reject any account opening application and/or commence / terminate the business relationship with a client.

The Company has employed a computerized system which assists the Company to identify and record the clients' identities, handle transactions and monitor clients' activities. The staff are required to upload the client's identification documents, transaction documents, compliance verified records, and other relevant documents to the system on a timely basis.

Travel Rule Requirements

The travel rule is the requirement to ensure that specific information (listed below) is included with the information sent or received in an Electronic Funds Transfer ("EFT") or a Virtual Currency ("VC") transfer.

Information received under the travel rule cannot be removed from a transfer.

The Company must include the travel rule information when it initiates an EFT for which an EFT record must be kept.

(a) the name, address and account number or other reference number (if any) of the person or entity who requested the transfer (originator information);
(b) the name and address of the beneficiary; and
(c) if applicable, the beneficiary's account number or other reference number.

The Company must also take reasonable measures to ensure that the travel rule information is included when it receives an EFT, either as an intermediary or as the final recipient. When sending an incoming or outgoing EFT (after receiving it as an intermediary), the Company must include the travel rule information it received or obtained through reasonable measures.

Large Cash Transaction Report or large cash transaction record

The Company must submit a Large Cash Transaction Report to FINTRAC when it receives $10,000 (or foreign currency equivalent to $10,000) or more in cash in a single transaction from a person or entity.

Cash includes:

(a) coins and bank notes issued by the Bank of Canada that are intended for circulation in Canada
(b) coins and bank notes of countries other than Canada
(c) fiat currency

Cash does not include:

(a) other forms of funds such as cheques, money orders or other similar negotiable instruments
(b) virtual currency

The Company must also submit a Large Cash Transaction Report to FINTRAC in accordance with the 24-hour rule. That is, it must submit a report when:

(a) it receives 2 or more amounts in cash that total $10,000 or more within a consecutive 24-hour window, and
(b) it knows that the transactions are:
    (i) conducted by the same person or entity
    (ii) conducted on behalf of the same person or entity (third party), or
    (iii) for the same beneficiary

Ref: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/lctr-doie/lctr-doie-eng

When the Company submits a Large Cash Transaction Report (LCTR), it must take reasonable measures to determine whether the person that gave it the cash is acting on behalf of a third party.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/tpdr-eng

Record Keeping

Maintaining complete and accurate records is foundational for a financial institution's compliance. This is not only about fulfilling our legal obligations but also about providing transparency for clients and shareholders and supporting audits and internal controls. The Company is committed to ensuring all records are properly and securely retained, supporting compliance efforts and providing the highest level of trust for our clients, shareholders, and partners. The Company shall keep the documents obtained in the course of identifying and verifying the identity of the client and maintain the documents obtained in connection with the transactions.

The Company's Record Keeping Strategy:

(a) Completeness: All transaction and communication records related to anti-money laundering activities will be fully retained, including but not limited to client KYC information, transaction records, internal and external communication records, and due diligence results.

(b) Security: The Company uses the most advanced encryption and backup technologies to ensure these records are not lost, tampered with, or accessed by unauthorized third parties.

(c) Accessibility: While records will be securely stored, the Company ensures that they can be quickly and easily accessed when needed, such as for legal requirements or internal audits.

The Company should keep:

(a) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the client (including each partner, director, officer and authorized signatory of an entity) and/or beneficial owner of the client and/or beneficiary and/or persons who purport to act on behalf of the client and/or other connected parties to the client;

(b) other documents and records obtained throughout the CIV and ongoing monitoring process, including Enhanced Measures;

(c) where applicable, the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship; and

(d) the original or a copy of the records and documents relating to the client's account (e.g., account opening form; or risk assessment form) and business correspondence with the client and any beneficial owner of the client (which at a minimum should include business correspondence material to CIV measures or significant changes to the operation of the account); and

(e) the results of any analysis undertaken (e.g., inquiries to establish the background and purposes of transactions that are complex, unusually large in amount or of unusual pattern, and have no apparent economic or lawful purpose).

In order to comply with the above requirements, all records of transactions and clients must be filed and uploaded to the system on a timely basis for complete recording and clearing.

The purpose of keeping records is to ensure that we can keep track on Clients with business relationship and their transactions. The records will enable the Company to keep track of their trading sums, frequencies and where funds are remitted to, and currencies exchanged and see if their trading records are consistent with their descriptions at the time of account opening or whether any transaction may possibly be considered suspicious.

The Company will comply with the law and maintain client records for at least five years after the end of the business relationship. The Company will also maintain transaction records for at least five years after the completion of a transaction, regardless of whether the business relationship ends during the period. The staff shall ensure that all records are properly completed and filed with the accounts department and uploaded to the computerized system on a timely basis.

The Company will comply with the law and provide any client and transaction information to the relevant authorities as and when demanded, or under specific circumstances stated in the law. All correspondence / reports, both internal or with the appropriate authority, in connection with suspicious transactions must be retained for a minimum period of at least five years after the relevant authority has closed the case.

Ongoing Monitoring

Ongoing monitoring is a process that the Company must develop and use to review all the information it has obtained about the clients with whom it has a business relationship, in order to:

(a) detect any suspicious transactions that it is required to report to FINTRAC;
(b) keep client (including each partner, director, officer and authorized signatory of an entity) identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
(c) reassess the level of risk associated with its client's transactions and activities; and
(d) determine whether transactions or activities are consistent with the client information it obtained and its risk assessment of the client.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/omr-eng

The Company adopts a risk-based approach to adopt appropriate controls and oversight and accordingly to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

The Company shall continuously monitor its business relationship with client by:

(a) reviewing from time-to-time documents, data and information relating to the client and obtained documents and information to ensure that they are up-to-date and relevant;

(b) monitoring the transactions (including cash and non-cash transactions) of the client by conducting appropriate scrutiny of transactions carried out for the client to ensure that they are consistent with the Company's knowledge of the client, the client's business, risk profile and source of funds; and

(c) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF and examining the background and purposes of those transactions and setting out the findings in writing.

The Company shall consider monitoring the following:

(a) the nature and type of transactions (e.g., abnormal size or frequency);

(b) the nature of a series of transactions (e.g., a number of cash deposits);

(c) the amount of any transactions, paying particular attention to particularly substantial transactions;

(d) the geographical origin/destination of a payment or receipt; and

(e) the client's normal activity or turnover.

When considering how to monitor client transactions and activities, the Company shall take into account the following factors:

(a) the size and complexity of its business;

(b) its assessment of the ML/TF risks arising from its business;

(c) the nature of its systems and controls;

(d) the monitoring procedures that already exist to satisfy other business needs; and

(e) the nature of the products and services (which includes the means of delivery or communication).

The Company shall undertake ad hoc review of the client records upon certain trigger events and periodic review at least every two years, including:

(a) when a significant transaction is to take place;

(b) when a material change occurs in the way the client's account is operated;

(c) when the Company client documentation standards change substantially; or

(d) when the Company is aware that it lacks sufficient information about the client concerned.

The Company shall undertake periodic review at least every year for high-risk clients, and at least every two years for medium or low-risk clients.

The Compliance Officer shall be responsible for informing the Senior Management on a timely basis if Compliance Officer suspects the transaction and/or client involves in any money laundering or Financing of

Terrorist activities, or with any high-risk indicators identified. The Senior Management shall have the authority to accept / reject any transaction and/or maintain / terminate the business relationship with a client.

The Compliance Officer shall be responsible for the execution and implementation of the Regulations issued by the Government of Canada and the Company's Compliance Program. Upon obtaining approval from the Senior Management, the Compliance Officer shall also be responsible for reporting any suspicious transactions directly to the Compliance Officer. The Compliance Officer shall take instructions from the CO and shall report to him on all matters regarding compliance.

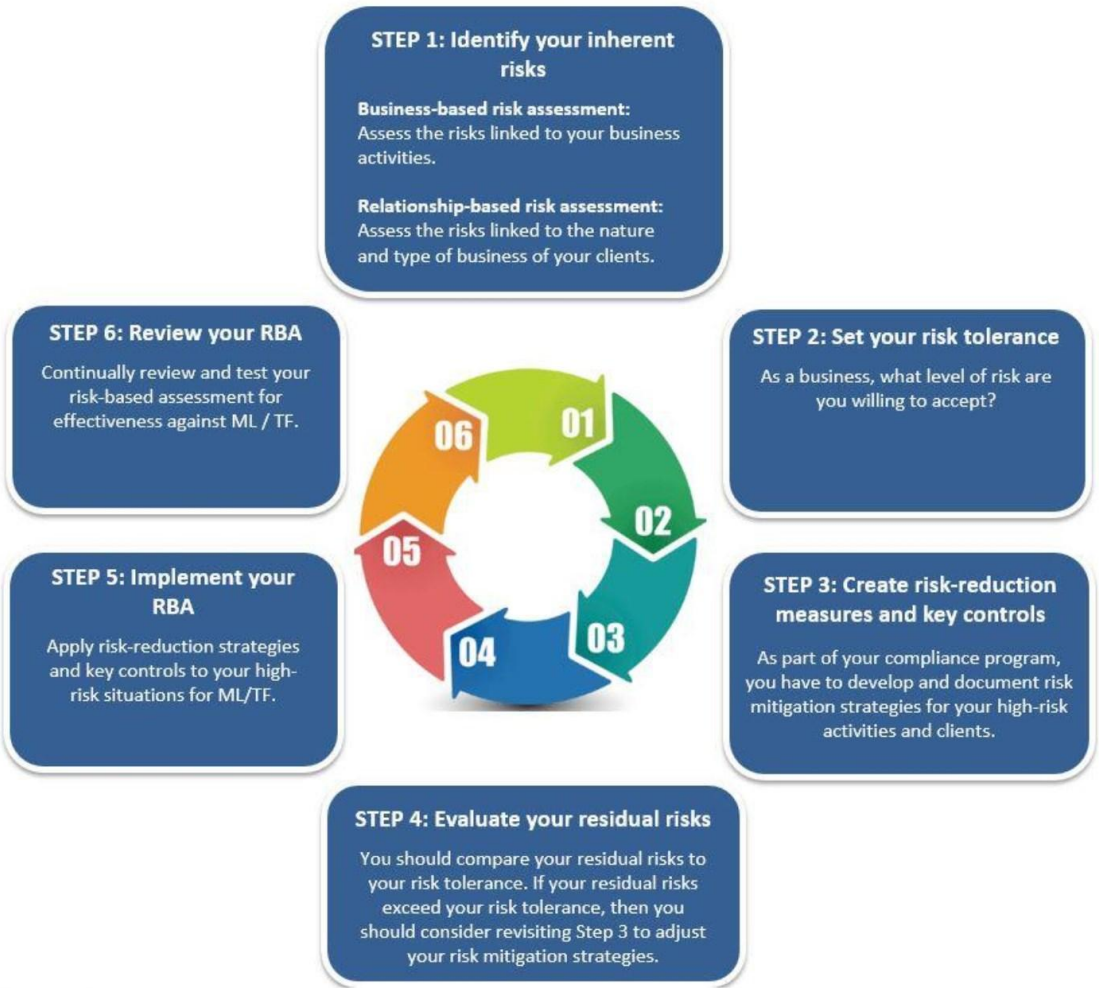
The computerized system will assist in client screening on a periodic basis and in receiving notification from CCE regarding the latest news and regulations of the Company.

Paragraph 5: Risk Identification, Business-based Risk Assessment (BRA) and Client Risk Assessment (CRA)

Risk Identification

Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. A Risk Based Approach ("RBA") is a way for the Company to conduct its risk assessment by considering elements of its business, clients and/or business relationships to identify the impact of possible ML/TF risks, and to apply controls and measures to mitigate these risks.

Diagram 1: RBA cycle



Business-based Risk Assessment ("BRA")

A BRA allows the Company to identify, assess and understand the ML/TF risks in relation to:

(a) The combination of its products, services and delivery channels;
(b) The geographical locations in which its business operates;
(c) The impact of new developments and technologies that affect its operations;
(d) The risks that result from affiliates (the activities that they carry out); and
(e) Other relevant factors.

The Company will identify, assess and understand the ML/TF risks to which it is exposed and takes AML/CFT measures commensurate with those risks in order to manage and mitigate them effectively. The Company will adopt an RBA in the design and implementation of its AML/CFT Systems with a view to managing and mitigating ML/TF risks.

The Company will take the following steps to conduct the institutional ML/TF risk assessment:

(a) identified and documented all the inherent risks to its business (e.g., using a business-based risk assessment worksheet)
(b) assign a level or score to each risk using an appropriate scale or scoring methodology
(c) setting the Company's risk tolerance
(d) creating risk-reduction measures and key controls
(e) evaluating its residual risks
(f) implementing its RBA
(g) reviewing its RBA

Ref: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/rba/rba-eng

The Company will conduct its assessment every two years and upon trigger events which are material to the Company's business and risk exposure.

Client Risk Assessment

The Company conducts CRA to assess the ML/TF risks associated with the clients in order to differentiate between the risks of individual clients and business relationships, as well as apply appropriate and proportionate CIV and risk mitigating measures.

The Company applies Enhanced Measures and on-going monitoring to manage those clients with higher risks and knows that simplified due diligence measures may be applied to clients with lower risks.

The Company applies a risk-based approach to assessing which clients are to be of higher risk of ML/TF. The followings are some risk factors to be identified:

1. Types of clients and behaviour
2. Products and services offered
3. Delivery channels
4. Client's business organisation/geographical locations involved

Examples of potentially higher risk factors in ML/TF are:

(a) client risk factor:

(i) business relationship is conducted in unusual circumstances (e.g., significant unexplained geographic difference between the Company and the client, defined groups of individuals conducting transactions at single or multiple locations or across multiple services);

(ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;

(iii) companies that have nominee shareholders, nominee directors, bearer shares or bearer shares warrants;

(iv) client owns or operates cash intensive business;

(v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business;

(vi) client knows little or is reluctant to disclose details about the recipient/ originator; or

(vii) the client (including each partner, director, officer and authorized signatory of an entity) or the beneficial owner of the client is a politically exposed person.

(b) product, service, transaction or delivery channel risk factors:

(i) anonymous transactions (which may involve cash);

(ii) structured transaction in an apparent attempt to break up amounts to stay below any applicable threshold for CIV or the special requirements for remittance transactions as stated in Chapter 11, which has an effect of avoiding CIV and/or record keeping;

(iii) transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;

(iv) frequent payments received from unknown or un-associated third parties;

(v) client involves in transactions that have no apparent ties to the destination/origination jurisdiction and with no reasonable explanations;

(vi) transaction volume of agents or counterparts of Company is inconsistent with either overall or relative to typical past transaction volume; or

(vii) agents that operate sub-standard compliance programmes.

(c) country risk factors:

(i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed

assessment reports, as not having effective AML/CFT Systems;

(ii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

(iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or

(iv) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.

Enhanced measures

Enhanced measures are the additional controls and processes that the Company put in place to manage and reduce the risks associated with its high-risk clients and business areas. As part of its compliance program, the Company must develop and apply written policies and procedures for the enhanced measures that it will take for any ML or TF risks it identifies as high.

The Company's policies and procedures for enhanced measures must include:

(a) the additional steps, based on assessment of the risk, that it will take to verify the identity of a person or entity; and

(b) any other additional steps that it will take to mitigate the risks, including, but not limited to, the additional steps to:

(i) ensure client (including each partner, director, officer and authorized signatory of an entity) identification information and beneficial ownership information is updated at a frequency that is appropriate to the level of risk; and

(ii) conduct ongoing monitoring of business relationships at a frequency that is appropriate to the level of risk.

Examples of possible Enhanced Measures include:

(a) obtaining additional information on the client (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and using the information to inform the client risk profiling as well as updating more regularly the identification data of client (including each partner, director, officer and authorized signatory of an entity) and beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds and source of wealth of the client;

(d) obtaining information on the reasons for attempted or conducted transactions;

(e) evaluating the information provided by the client with regard to destination of funds involved in the transaction and the reason for the transaction to better assess the risk of ML/TF; or

(f) requiring the first payment to be carried out through an account in the client's name with a bank subject to

similar CIV standards.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s5

Source of wealth refers to the origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc.

Source of funds refers to the origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/glossary-glossaire/1-eng#sourcevc

Simplified identification method

The Company may use the simplified identification method to meet its obligation to verify the identity of a corporation or other entity. Specifically, it is deemed to comply with its requirement to verify the identity of a corporation or other entity if, based on its risk assessment, it considers there is a low risk of a money laundering offence or terrorist activity financing offence, and if:

- the corporation or other entity whose identity is being verified:
  (a) is referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;
  (b) is a foreign corporation or entity that carries out activities that are similar to those of an entity referred to in any of paragraph 5(a) to (g) of the PCMLTFA;
  (c) administers a pension or investment fund that is regulated under the legislation of a foreign state and that either is created by a foreign government or is subject to the supervision of a competent authority under the legislation of that foreign state;
  (d) is one whose shares are traded on a Canadian stock exchange, or a stock exchange designated under subsection 262(1) of the Income Tax Act;
  (e) is a subsidiary of a corporation or an entity that is referred to in paragraphs a. to d. in this section, and is one whose financial statements are consolidated with the financial statements of that corporation or entity;
  (f) is an institution or agency of, or in the case of a corporation, is owned by, the government of a foreign state; or
  (g) is a public service body, as defined in subsection 123(1) of the Excise Tax Act; and
- the Company is satisfied that, within the applicable time period for which it had to verify identity, as explained in the sector-specific guidance on “When to verify the identity of persons and entities), the

corporation or other entity exists and that every person who deals with it on behalf of the corporation or other entity is authorized by it to do so.

If the Company subsequently considers, based on its risk assessment, that the risk of a money laundering offence or terrorist activity financing offence has increased and is no longer low then it must, as soon as feasible, verify the identity of the corporation or other entity, as the case may be, by referring to the appropriate records.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s73

If the Company uses the simplified identification method to verify the identity of a corporation or other entity, it must keep a record that sets out:

(a) the grounds for considering there is a low risk of a money laundering offence or terrorist activity financing offence; and

(b) the information obtained about the corporation or other entity, as the case may be, and about the persons that assure the Company that the corporation or other entity exists and that the persons the Company deals with are authorized to act on behalf of the corporation or the entity.

In particular, the Company does not accept any person / corporation involving in the following business as clients or carry out transactions involving these activities:

(a) Casino
(b) Online gaming
(c) Military
(d) Armory
(e) Any illegal activities
(f) Virtual currencies trading

For verification of the identity of a client (including each partner, director, officer and authorized signatory of an entity) and any beneficial owner of the client after establishing the business relationship, the Company will adopt appropriate risk management policies and procedures concerning the conditions under which the client may utilise the business relationship prior to verification. These policies and procedures include:

(a) the identity verification measures and the follow-up actions should be completed as soon as possible. The client relationship will be suspended if the verification cannot be completed within 30 days and terminated if the verification cannot be completed within 120 days;

(b) all subsequent transaction before the completion of verification shall be approved by senior management or CO;

(c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship;

(d) keeping senior management periodically informed of any pending completion cases; and

(e) ensuring that funds are not paid out to any third party.

Exceptions may be made to allow payments to third parties subject to the following conditions:

(i) there is no suspicion of ML/TF;

(ii) the risk of ML/TF is assessed to be low;

(iii) the transaction is approved by senior management, who should take account of the nature of the business of the client before approving the transaction; and

(iv) the names of recipients do not match with watch lists such as those for terrorist suspects and politically exposed persons (PEPs).

If the Compliance Officer believes the circumstances to be suspicious, the Compliance Officer should report the matter to the appropriate authorities.

Paragraph 6: Staff Awareness to Anti-Money Laundering and Counter-Financing of Terrorist

The Company recognizes the importance of Training in the complex and ever-changing financial sector. Training and education are key to ensuring the Company's team always stays ahead, prevents financial crimes, and maintains market stability. Professional, continuous, and in-depth training is the cornerstone to ensure that the Company always meets the highest standards of the financial industry.

The Company believes in the power of the team. The Company is committed to cultivating a risk control and anti-money laundering team with deep professional knowledge and excellent teamwork spirit. Through continuous communication and collaboration, the Company ensures that every member can provide the best protection for clients and the market at the forefront of combating financial crimes.

The Company provides ongoing training to all relevant staff (including new staff) in order to ensure they are made aware of the PCMLTFA and the Company's AML/CFT systems. The Company also provides appropriate AML/CFT training to them regularly facilitating them to identify suspicious activities / transactions. The format of training includes:

(a) Systematic Training: The Company provides employees with a comprehensive AML training course, ensuring they not only understand the latest regulatory requirements but can also implement these provisions in practice.
(b) Practical Simulations: By simulating real financial crime scenarios, employees can quickly identify and address various risks in their actual work.
(c) External Expert Lectures: The Company regularly invites authoritative experts in the international anti-money laundering and risk control fields to train the team, ensuring their knowledge remains consistent with international best practices.
(d) Continuing Education: In addition to regular internal training, the Company encourages employees to attend external professional seminars, studies, and courses to continuously expand their knowledge horizons.

The Company will keep training records/records of relevant courses or seminars attended for a minimum of 3 years and for inspection by regulator, including records on:

(a) training date
(b) training recipients;
(c) training topics and materials;
(d) training methods for delivery; and
(e) training frequency.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s6

The Company will provide not less than 12 hours of one-to-one initial training to new staff as soon as possible after they are being hired or appointed. The Company will also provide not less than 3 hours training (e.g., seminar/workshop/self-learning/etc.) in every six months (i.e., minimum 6 hours annually) refresher training regularly to ensure that its staff are reminded of their responsibilities and are kept informed of new developments related to ML/TF, including:

(a) the Company's and their own personal statutory obligations and the possible consequences for failure to comply with CIV and record-keeping requirements under the PCMLTFA;

(b) the Company's and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions;

(c) any other statutory and regulatory obligations that concern the Company's and themselves under the PCMLTFA and other relevant regulations, and the possible consequences of breaches of these obligations;

(d) the Company's AML/CFT systems, including suspicious transaction identification and reporting; and

(e) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their particular roles in the Company's with respect to AML/CFT.

In particular, training will be arranged for:

(a) all new staff, who are required to attend initial training as soon as possible after being hired or appointed, irrespective of seniority:

(i) an introduction to the background to ML/TF and the importance placed on ML/TF by the Company; and

(ii) the need for identifying and reporting of any suspicious transactions to the CO, and the offence of "tipping-off";

(b) members of staff who are dealing directly with the public (e.g., front-line personnel):

(i) the importance of their roles in the Company's ML/TF strategy, as the first point of contact with potential money launderers;

(ii) the Company's policies and procedures in relation to CIV and record-keeping requirements that are relevant to their job responsibilities; and

(iii) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;

(c) back-office staff, depending on their roles:

(i) appropriate training on client verification and relevant processing procedures; and

(ii) how to recognise unusual activities including abnormal settlements, payments or delivery instructions;

(d) managerial staff including internal audit officers and COs:

(i) higher level training covering all aspects of the Company's AML/CFT regime; and

(ii) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the FINTRAC; and

(e) COs:

(i) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the FINTRAC; and

(ii) training to keep abreast of AML/CFT requirements/developments generally.

Paragraph 7: Reporting Suspicious Activities/Transactions

In the global financial ecosystem, the detection and reporting of suspicious activities occupy a central position. It not only helps prevent financial crimes, money laundering, and terrorist financing activities but is also key to ensuring the stability, fairness, and transparency of the financial market. Properly identifying and promptly reporting these activities is the cornerstone of protecting institutions from legal and reputational risks and ensuring the rights of financial consumers.

The Company will give sufficient guidance to all relevant staff to enable them to take appropriate actions when detecting suspicious transactions and to report the suspicious activities/transactions to CO as soon as possible.

A suspicious transaction report (STR) is a type of report that must be submitted to FINTRAC by the Company if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted in the course of its activities is related to the commission or the attempted commission of an ML/TF offence. Reference should be made to the list of ML/TF indicators issued by FINTRAC.
Ref: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/msb_mltf-eng

How to Detect and Report Suspicious Activities:

(a) Real-time Monitoring: Use cutting-edge financial technology tools, such as artificial intelligence and machine learning, to monitor client transactions in real-time, quickly identifying behaviors inconsistent with the client's historical transaction patterns.
(b) Regular Review: Conduct a systematic review at least once a year, analyzing client transaction patterns to ensure ongoing compliance.
(c) Internal Procedures: When behaviors inconsistent with regular transaction patterns are discovered, the relevant department must immediately conduct an internal review and record the findings in detail.
(d) Prompt Reporting: Once confirmed as suspicious activity, report promptly as per the FINTRAC regulations. The Compliance Officer will maintain close communication with FINTRAC and provide all necessary transaction information.
(e) Employee Training and Culture Building: Regularly provide training for employees on financial crime trends, encouraging them to report suspicious behaviors promptly and accurately.

The Company may adopt, where applicable, the “SAFE” approach, which includes: (a) Screening the account for suspicious indicators; (b) Asking the clients appropriate questions; (c) Finding out the client’s records; and (d) Evaluating all the above information. However, if any investigation, including but not limited to reaching the client, may raise concerns of tipping off the client, the investigation must not be implemented.

The CO shall be responsible for consolidating relevant information and/or documents in relation to suspicious activities/transaction and perform an investigation on the issue. If, after an investigation of the evidence, the CO is still in doubt, the CO should report the issue to the Senior Management. The Senior Management shall have the authority to decide if a Suspicious Transaction Report should be filed to FINTRAC by the Compliance Officer. Such a Suspicious Transaction Report should be filed with FINTRAC on a timely basis.

The Company shall maintain a record of all disclosures made to FINTRAC. The record shall include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located.

Paragraph 8: Internal Monitoring and Review System

As the financial market evolves, regulations, laws, and best practices change. To ensure that the Company always remains at the forefront of the industry and maintains its top-tier financial service standards, it is crucial to regularly review and update our Compliance Program.

A two-year effectiveness review is an evaluation that must be conducted every two years (at a minimum) to test the effectiveness of the elements of the Company's Compliance Program (policies and procedures, risk assessment, and ongoing training program and plan). The Company must start its effectiveness review no later than two years (24 months) from the start of the previous review. The Company must also ensure that it has completed its previous review before it starts the next review.

The purpose of an effectiveness review is to determine whether the Company's Compliance Program has gaps or weaknesses that may prevent its business from effectively detecting and preventing ML/TF. The effectiveness review will help the Company determines if:

(a) its business practices reflect what is written in its compliance program documentation and if it is meeting the requirements under the PCMLTFA and associated Regulations.

(b) its risk assessment is effective at identifying and mitigating the ML/TF risks related to its clients, affiliates (if any), products, services, delivery channels, new developments or technology, and geographic locations where it carries out its business.

The review must be carried out and the results documented by an internal or external auditor, or by the Company itself if it does not have an auditor. The review should be conducted by someone who is knowledgeable of the Company's requirements under the PCMLTFA and its associated Regulations. Also, as a best practice, to ensure that the review is impartial, it should not be conducted by someone who is directly involved in the Company's Compliance Program activities. Regardless of who carries out the review, as an RE it is the Company's responsibility to ensure that the review is conducted (at a minimum) every two years and that the review tests the effectiveness of its compliance program.

The Company must also institute and document a plan for the two-year effectiveness review of its Compliance Program. This plan should describe the scope of the review and must include all the elements of its Compliance Program. The breadth and depth of review for each element may vary depending on factors such as the complexity of its business, transaction volumes, findings from previous reviews, and current ML/TF risks. The plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation.

The Company may include the following areas (if appropriate) in the review:

(a) interviews with those handling transactions to evaluate their knowledge of its policies and procedures and related record keeping, client identification and reporting requirements;
(b) a review of a sample of its records to assess whether its client identification policies and procedures are being followed;
(c) a review of its agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that its agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed;
(d) a review of transactions to assess whether suspicious transactions were reported to FINTRAC;
(e) a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines;
(f) a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to RE sectors that have EFT obligations);
(g) a review of a sample of its client records to see whether the risk assessment was applied in accordance with its risk assessment process;
(h) a review of a sample of its client records to see whether the frequency of its ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment;
(i) a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken;
(j) a review of a sample of its records to confirm that proper record keeping procedures are being followed;
(k) a review of its risk assessment to confirm that it reflects its current operations; and
(l) a review of its policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect its current business practices.

The Company will document the following in its two-year effectiveness review report:

(a) the date the review was conducted, the period that was covered by the review and the person or entity who performed the review;
(b) the results of the tests that were performed; and
(c) the conclusions, including deficiencies, recommendations and action plans, if any.

A review report will be submitted to a senior officer no later than 30 days after the completion of the effectiveness review:

(a) the findings of the review (for example, deficiencies, recommendations, action plans);

(b) any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself; and
(c) the status of the implementation of the updates made to its policies and procedures.

Ref: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s7

The Company's Updating Policies:

(a) Quick Response: Apart from the annual review, the Company will continuously monitor financial regulations. Upon identifying new regulations or best practices, the Company will swiftly act to make necessary updates to the policy.
(b) Internal Notification: After each policy update, all relevant departments and employees will be immediately notified, ensuring everyone is aware of and complies with the latest provisions.

The Company views review and update as core components to ensure our service quality and protect client interests. The Company commits that, regardless of how the financial environment changes, policies and practices will always meet the highest possible standards.

Internal controls form the frontline defense against improper operations, fraud, and other risks. The Company believes that a robust and effective internal control system is the cornerstone to ensure the Company adheres to the Compliance Program, protect client funds, and maintain the Company's reputation.

The Company's Internal Control Strategy:

(a) Continuous Monitoring: The Company has a dedicated team responsible for real-time monitoring of various transaction activities, ensuring company activities align with the AML/CTF systems.
(b) Multi-level Review: To reduce errors and omissions, all key operations and decisions require multi-level reviews.
(c) Technological Support: The Company invests in advanced monitoring and auditing technologies, ensuring the Company can quickly and effectively identify any potential non-compliance.

The Company's Handling Non-compliance:

(a) Immediate Response: Once any non-compliance with the Compliance Program is identified during the audit process, the Company will immediately take corrective measures.
(b) Disciplinary Measures: Depending on the severity of the non-compliance, the Company will take appropriate disciplinary actions, ranging from verbal warnings to termination of employment.
(c) Continuous Improvement: Every identified non-compliance is seen as an opportunity for improvement. The Company will analyze the cause, update processes, and ensure the same issue does not recur.

Paragraph 9: Other Statutory Requirements

The Company establishes and maintains effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on ML/TF. The legal and regulatory obligations of the Company and those of the staff are well understood and adequate guidance and training are provided to the staff.

The Company maintains a database or subscribe to a database maintained by a third-party service provider of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to the Company and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database. An effective screening mechanism is implemented to avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties.

The purpose of this Compliance Program is to highlight some particular areas of the relevant statutory provisions and this policy will be always read in conjunction with the PCMLTFA. The Company shall implement the above policy, procedures and controls to mitigate the risks of money laundering and Financing of Terrorist.

This Compliance Policy is established and approved by the Board of Director of the Company.

_____

Name of Signatory:

Date:

Annex

Summary of the methods to identify persons and associated record keeping obligations

Identification method	Documents or information to review	Identification details that must match	Information that must be recorded
Government-issued photo identification	Photo identification document issued by a government (not a municipal government) that is authentic, valid and current	Name and photograph	• Person's name • Date of verification • Type of document • Document number • Province or state and country that issued the document • Expiry date (if applicable)
Credit file	Valid and current information from a Canadian credit file that has been in existence for at least three years where information is derived from more than one source	Name, address and date of birth	• Person's name • Date consulted/searched the credit file • Name of the credit bureau or third-party vendor • Person's credit file number
Dual-process	Valid and current information from two different reliable sources where neither the RE nor the person is a source	A combination of two of the following: • name and address; • name and date of birth; **or** • name and confirmation of a	• Person's name • Date verified the information • Name of the two different sources used to verify the identity of the person • Type of information referred to • Account number or

		financial account	number associated with the information if no account number exists
Affiliate or member	Information in the records of the affiliate or the member for the method used	Name, address and date of birth	• Person's name • Date verified the identity of the person • Name of affiliate or member that previously verified the identity of the person • Method used by the affiliate or member to verify the person's identity • Information that the affiliate or member recorded based on the method used
Reliance	• Be satisfied that the information from the other RE or affiliated foreign entity is valid and current, and that the person's identity was verified by using the government-issued photo identification, credit file or dual-process methods or • Where the identity was verified prior to June 1, 2021, that	The identification details listed under the identification method used	• Person's name • The written agreement or arrangement with the other RE or affiliated foreign entity for the purpose of verifying a person's identity • The information provided by the other RE or affiliated foreign entity that they referred to in order to verify the identity of the person

	the person's identity was verified using one of the methods in force in the PCMLTFR at that time		

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#annex1

Annex

Summary of methods to identify an entity and associated record keeping obligations

Identification Method	Documents or information to review	Identification details that must match	Information that must be recorded
Confirmation of existence	• Information that is authentic, valid and current **For an entity (other than a corporation):** • partnership agreement • articles of association • the most recent version of any other record that confirms its existence and contains its name and address **For a corporation:** • certificate of incorporation • record that has to be filed annually under provincial securities legislation • the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors	• Name and address • Names of Directors (for corporation only)	If consulted an electronic record from a publicly accessible database: • registration number; • type of document consulted; and • source of the electronic document. If consulted a paper record or an electronic record: • the paper record, or a copy of the record.
Reliance	• Verify that information	• Name and	• Entity's name

	from the other RE or affiliated foreign entity is valid and current, and that the entity's identity was verified by using the confirmation of existence method • Where the identity was verified prior to June 1, 2021, that the entity's identity was verified using one of the methods in force in the PCMLTFR at that time	address • Names of Directors (for corporation only)	• The written agreement or arrangement with the other RE or affiliated foreign entity for the purpose of verifying an entity's identity • The information provided by the other RE or affiliated foreign entity that they referred to in order to verify the identity of the entity
Simplified identification	• Risk assessment to confirm that the risk of a money laundering offence or terrorist activity financing offence is low • Information to satisfy that the entity exists and that every person who deals with the Company on behalf of the entity is authorized to do so	N/A but this method can only be used to verify the identity of specific entities	• The grounds for considering that there is a low risk of a money laundering offence or terrorist activity financing offence • The information obtained about the entity and persons to satisfy that it exists and that the persons the Company deals with are authorized to act on behalf of the entity

Ref: https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#annex3

Annex

Prohibited Jurisdictions

The Company will not process any transaction related to any of the following jurisdictions:

1. Democratic People's Republic of Korea (DPRK)
2. Islamic Republic of Iran (Iran)
3. Albania
4. Barbados
5. Burkina Faso
6. Cayman Islands
7. Democratic Republic of the Congo
8. Gibraltar
9. Haiti
10. Jamaica
11. Jordan
12. Mali
13. Mozambique
14. Nigeria
15. Panama
16. Russia
17. Senegal
18. South Africa
19. South Sudan
20. Syria
21. Tanzania
22. Turkey
23. Uganda
24. United Arab Emirates
25. Yemen

Ref:
https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2023.html

Annex

Prohibited Industries

The Company will not process any transaction related to any of the following industries:

(a) Casino

(b) Online gaming

(c) Military

(d) Armory

(e) Any illegal activities

(f) Virtual currencies trading