PALMEX GROUP INC
ANTI-MONEY LAUNDERING &
COUNTER TERRORIST FINANCING POLICY

Implementation Date: August 2025

Version Number: 1.0

Last Updated: August 2025

Next Update: August 2026

Approved By: Petros Kattou, Compliance Officer

Senior Officer Approval for Program: Petros Kattou, Director

Document Classification: Confidential

Table of Contents

1 Policy Statement

1.1 Our Commitment

PALMEX GROUP INC (Palmex) is committed to preventing, detecting and deterring money laundering and terrorist financing and has a zero-tolerance policy in regard to money laundering and terrorist financing. To that end, it is the responsibility of every employee (including contract and part-time employees) to comply with this program and all related Canadian legislation.

While Palmex is committed to having an effective compliance program in place, if we become aware of a non-compliant event, a voluntary self-declaration of non-compliance will be made FINTRAC.

Our procedures for implementing this policy are described in separate documents, as is our Risk Assessment. This policy pertains to Anti-Money Laundering (AML) obligations in Canada only. Other AML obligations that we may have to comply with, based on jurisdictions we operate in, are contained in separate documents.

To be read in addition to this policy, specific procedures have been designed for:

- All Staff, and
- Compliance Staff.

This policy applies to all individuals working at all levels of Palmex including directors, senior managers, officers, employees, consultants, contractors, part-time and fixed-term workers and casual staff, all of whom are collectively referred to as 'staff' in this document.

Every staff member of Palmex receives, at a minimum, annual basic AML / & Counter Terrorist Financing (CTF) training as well as the anti-fraud and anti-bribery.

1.2 Anti-Bribery

Palmex is committed to conducting business in an ethical and honest manner and is committed to implementing and enforcing systems that ensure bribery is prevented. Palmex has zero-tolerance for bribery and corrupt activities. We are committed to acting professionally, fairly, and with integrity in all business dealings and relationships, wherever we operate.

1.3 Canadian Regulatory Background & Context

On July 10, 2019, an amendment to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its enacted regulations was published. The amended regulations state that persons or entities engaged in the business of exchanging, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another are considered FMSBs and MSBs, effective June 1, 2020.

Additional provisions, including the requirement to report large virtual currency transactions to FINTRAC and other virtual currency specific obligations set out in the regulations that became effective June 1, 2021.

1.4 Compliance Program

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its regulations (Regulations), FMSBs and MSBs are required to have an AML & CTF program[1] that consists of these five elements:

1) Written policies and procedures: these list our responsibilities under the law, and what we are doing to meet them;
2) A documented Risk Assessment: a document that describes and assesses the risk that our business could be used to launder money or finance terrorism;
3) The appointment of a Compliance Officer: the person who is ultimately responsible to develop and maintain our AML and CTF compliance program;
4) AML Compliance Effectiveness Reviews: testing and reporting completed either annually or every two years that assesses how well our compliance program is working; and
5) Training & Training Plan: training must be conducted at least annually to ensure that everyone understands their roles and responsibilities, and there must be a documented training plan in place for the training to be conducted.

These five elements are discussed in detail later in this policy.

1.5 Operational Compliance

In addition to our documented program that consists of the five elements, FMSBs and MSBs are required to operate in a compliant manner. This includes:

- Collecting and recording customer identification information;
- Know Your Customer (KYC) information;
- Transaction monitoring and customer risk scoring;
- Reporting certain transactions to regulators and government agencies;
- Complying with Ministerial Directives;
- Maintaining appropriate registration and licensing; and
- Keeping records.

The actions described in our procedures for this purpose are required (not optional) in all cases. Any activity that is offside with our AML and CTF procedures should be brought to the attention of the Compliance Officer immediately.

2 AML & CTF Basics

Money laundering is the process of taking money (including virtual currency) obtained by committing a crime and disguising the source to make it appear legitimate. Under the Criminal Code of Canada, it is illegal to launder money or to knowingly assist in laundering money. Under the PCMLTFA and Regulations, as well as legislation applicable in other jurisdictions in which we operate, we must take steps to be sure that our business is not used to launder money and if we suspect that money laundering may be taking place, we must report it.

Terrorist financing is the process of moving funds in order to pay for terrorist activities. Unlike money laundering, the source of the funds is not always criminal, but the intended use of the funds is criminal. Under the Criminal Code of Canada, it is illegal to knowingly assist in the financing of terrorism, including the possession of terrorist funds or property. If we know or suspect that we have terrorist property in our possession, it must be reported immediately.

2.1 How Money Laundering & Terrorist Financing Work

Money laundering is described as having three phases by the Financial Action Task Force ('FATF'). These are Placement, Layering and Integration.

Terrorist financing, as opposed to money laundering can, occur with legitimate funds (including virtual currency). Meaning; funds which are not the proceeds of crime. Legitimate funds can be transferred and used by those who would commit terrorist activities. In this, it can be said that terrorist financing most often acts in the 'Layering' and 'Integration' phases described by the FATF. But rather than luxury items, the funds are used for the commission or support of terrorist activities and/or organizations. These phases are described in detail below:

> **Placement:** In the initial, or placement stage of money laundering, the launderer introduces illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.
>
> **Layering:** After the funds have entered the financial system, the second, or layering stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Integration: Having successfully processed funds through the first two phases the launderer then moves them to the third stage, integration, in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

While it is useful to understand these stages, it is not necessary to identify the stage, or even to know that money laundering is taking place, to consider a transaction to be suspicious. It is enough to have "reasonable grounds to suspect" that money laundering may be occurring, based on the facts, context and indicators present. If something seems unusual, trust your instincts, and escalate the issue to the Compliance Officer. In any instance where there are reasonable grounds to suspect that a transaction may be related to money laundering or terrorist financing, it must be escalated to the Compliance Officer for review.

3 Canadian Regulatory Background & Requirements

3.1 Money Services Businesses

Based on our service offering to Canadians, Palmex is considered a Foreign Money Services Business (FMSB). FMSBs are considered reporting entities under the law in Canada. This means that we must comply with certain requirements and answer to our regulator if we conduct certain transactions. Our regulators, federally, define foreign MSB activity in the following way:

"You are considered to be a foreign money services business (FMSB) if any of the following apply:

1. You are engaged in the business of providing at least one money services business (MSB) service;
   - **Foreign exchange dealing** - conducting transactions where one type of money or currency (like US dollars, Canadian dollars, Euros and so on) is exchanged for another.
   - **Money transfer service** - transferring funds from one individual or entity to another using an electronic funds transfer network or any other transfer method such as hawala, hundi, fei ch'ien, and chiti.
   - **Cashing or selling money orders, traveller's cheques or anything similar** - this does **not** include cashing cheques made out to a particular individual or entity."
   - **Dealing in Virtual Currency** - means an exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another.

2. You do not have a place of business in Canada;
3. You direct your MSB services at persons or entities in Canada; and
4. You provide these services to customers in Canada."

In Québec, the additional activities that are included in the MSB Act are:

- **Cheque cashing** (including the types of activity that are excluded under the last point of the federal definition); and
- The **operation of automated teller machines**, including the leasing of a commercial space intended as a location for an automated teller machine if the lessor is responsible for keeping the machine supplied with cash.

3.2 FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[2] is the agency that regulates our industry to ensure that we are meeting our obligations. FINTRAC provides guidance on the obligations set out by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations, and how reporting entities such as Palmex should incorporate these obligations into their operations. They have the power to review our documentation and to levy significant penalties if we are not compliant. Individuals that deliberately attempt to circumvent the law may also be charged criminally in addition to monetary penalties.

FINTRAC is also Canada's financial intelligence unit (FIU). The agency receives reports from reporting entities, like us, about transactions and analyses the data that they receive. This data is used to assist law enforcement investigations into crimes related to money laundering and terrorist financing. It is vital to this process that the information that we submit to FINTRAC is accurate, on time and as complete as possible.

FINTRAC also requires FMSBs and MSBs to maintain an up to date MSB registration. This includes keeping information about our business activities, key persons and banking services relationships up to date. If there are any changes, we need to inform FINTRAC within 30 days. If our business stops operating in Canada, or no longer offer MSB services we must cancel our MSB registration.

3.3 Revenu Québec[3]

The Minister of Revenue and Revenu Québec assumed responsibility for the application of the Money-Services Businesses Act from the Autorité des marchés financiers (Revenu Québec) on September 13, 2021. Revenu Québec enforces Québec's Money-Services Business Act (MSB Act) and its enacted regulations. The MSB Act defines MSB's more broadly than the Canadian federal definition and includes provincial licensing and registration requirements.

[2] http://www.fintrac.gc.ca/

[3] Palmex does not currently conduct transactions that required registering with Revenu Quebec.

3.4 Provincial Securities Regulators[4]

Provincial bodies regulate securities dealers and derivatives markets. These bodies require reporting from FMSBs and MSBs that conduct foreign exchange transactions that meet the following criteria[5]:

- Settle over a period longer than 2 business days, and/or
- Contain a rollover provision, and/or
- Are conducted for the purpose of financial speculations (i.e., that are not conducted with an expectation of delivery of the physical currency).

These transactions are required to be reported to a local Trade Repository (TR) along with the Legal Entity Identifiers (LEIs) of all entities party to the transaction, the Unique Product Identifier (UPI) describing the type of product sold, and the Unique Transaction Identifier (UTI) attached to the particular transaction reported.

Additional guidance specific to virtual assets, including CSA Staff Notice 21-327 and 51-363. Notice 21-327 provides an example of situation where securities legislation does not apply:

- a Platform offers services for users to buy or sell Bitcoin and does not offer margin or leveraged trading;
- users send money to the Platform to purchase Bitcoin at a given price;
- the terms of the transaction require that the entire quantity of Bitcoin purchased from the Platform or counterparty seller be immediately transferred to a wallet that is in the sole control of the user, and the transfer is immediately reflected on the Bitcoin blockchain;
- there is no agreement, arrangement or understanding between the parties that would allow the transaction to be settled other than by immediate transfer of Bitcoin;
- the Platform's typical commercial practice is to make immediate delivery in accordance with the terms of the transaction, and for the Platform or its affiliates not to have ownership, possession or control of the user's Bitcoin at any point following the transaction;
- the sale or purchase of Bitcoin is not merely evidenced by an internal ledger or book entry that debits the seller's account with the Platform and credits the crypto assets to the user's account with the Platform, but rather, there is a transfer of the Bitcoin to the user's wallet; and

[4] Palmex does not currently conduct transactions that fall under securities requirements. Should we consider these types of activities at any time, the compliance program will be updated to include all relevant requirements before any qualifying products and/or services are offered.

[5] Some exemptions apply. The complete criteria may vary from province to province, despite the existence of standardized guidance at the federal level.

- the Platform or counterparty seller retains no ownership, possession or control over the transferred Bitcoin.

CSA Staff Notice 51-363 pertains to custody of virtual assets. Palmex holds custody of its own virtual currency assets and has appropriate controls in place (such as safeguarding of private keys) Palmex does not hold custody of customer funds, Palmex's business consists of an E-wallet that is available in both the Apple App and Google Play stores and enables our customers, to purchase virtual currencies such as Bitcoin and Ethereum using fiat rails such as credit card processing and other virtual currencies

Furthermore, on March 29, 2021, CSA Staff Notice 21-329 issued additional guidance for compliance with the regulatory requirements. The guidance stated that the two most common characteristics of a Crypto-Asset Trading Platform (CTP) that suggest it would be a Dealer Platform and not a Marketplace Platform are as follows:

- it only facilitates the primary distribution of Security Tokens, and
- it is the counterparty to each trade in Security Tokens and/or Crypto Contracts, and customer orders do not otherwise interact with one another on the CTP.

CTPs that are Dealer Platforms may also be engaged in other activities or perform other functions that marketplaces typically do not undertake. These include, but are not limited to:

- onboarding of retail customers onto the CTP,
- acting as agent for customers for trades in Security Tokens6 or Crypto Contracts, and
- offering custody of assets, either directly or through a third-party provider.

3.5 Regulator Examinations & Compliance Assessment Reports

FINTRAC is responsible for ensuring that we (as a reporting entity) are meeting our obligations. To do this, they will periodically request information. We may receive these requests by email, phone or in writing. All requests should be forwarded to the Compliance Officer for handling immediately.

Most requests will be time sensitive. This means that we only have a certain amount of time to reply by law. For most information requests, this is 30 calendar days. If we do not respond to these requests or respond late, we may be subject to penalties.

[6] The Staff Notice does not elaborate on what cryptoassets are considered securities under Canadian securities laws, but the CSA's previous guidance (In CSA Staff Notice 46-307 Cryptocurrency Offerings) set parameters for what may be considered a security.

3.6 Ministerial Directives

From time to time, the Minister of Finance will issue additional directives for AML reporting entities. The Compliance Officer will ensure that our policies, procedures and Risk Assessment are updated accordingly. This may include the implementation of new processes in order to comply with directives, and to test the effectiveness of compliance measures. The Compliance Officer will maintain an awareness of such directives by regularly reviewing FINTRAC's website[7] and subscribing to FINTRAC's mailing list[8].

Currently, there are two ministerial directives pertaining to transactions that originate from, or are destined to North Korea (also known as the Democratic People's Republic of Korea, or DPRK) and Iran (Islamic Republic of Iran). We do not serve North Korea, Iran or other regions noted in FINTRAC's operational briefs on the subject. As such, no additional mediation steps have been taken in this case.[9]

4 Roles & Responsibilities

Everyone at Palmex a responsibility to ensure that our AML and CTF compliance program runs smoothly.

- Senior Management & Board of Directors:
    - Overseeing the AML and CTF compliance program on a high level;
    - Receiving regular (at least annual) status reports on the AML and CTF compliance program;
    - Being accessible to the Compliance Officer as needed where AML or CTF related issues arise;
    - Ensuring that the Compliance Officer has the resources to run an effective AML and CTF compliance program;
    - Ensuring that the Compliance Officer is adequately qualified to manage the AML and CTF compliance program (understand Canadian AML and CTF requirements and the business model); and
    - Signing off on the results of completed AML Compliance Effectiveness Reviews (within 30 days of the issue of the report).

- Compliance Officer:
    - Developing and maintaining the AML and CTF Compliance Program and Risk Assessment, which includes regularly reviewing and updating these documents and maintaining a record of all updates;
    - Ensuring that all employees and other relevant parties received appropriate AML and CTF training at least annually;

[7] http://www.fintrac.gc.ca/obligations/directives-eng.asp
[8] http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp
[9] https://www.fintrac-canafe.gc.ca/obligations/dir-dprk-eng and https://www.fintrac-canafe.gc.ca/obligations/dir-iri-eng

- Reporting the Senior Management and the Board of Directors (if applicable) on the status of the AML Program, including any AML Compliance Effectiveness Reviews (within 30 days of the issue of the report) and regulatory examinations;
- Overseeing AML Compliance Effectiveness Reviews and ensuring that the reviewer has sufficient knowledge of Canadian AML and CTF requirements and our business to conduct the review;
- Maintaining complete and accurate records;
- Maintaining up to date registration with FINTRAC;
- Maintaining up to date licensing with the Revenu Québec;
- Corresponding with FINTRAC and the Revenu Québec;
- Maintaining up to date knowledge of Canadian AML and CTF requirements as they apply to our business model; and
- Obtaining appropriate training, including continuing education, in order to develop and maintain knowledge of AML and CTF compliance requirements and industry best practices.

- All Employees:
  - Complying with the requirements set out in the AML and CTF compliance program;
  - Reporting certain types of transactions to the Compliance Officer;
  - Keeping up to date and accurate customer records;
  - Obtaining customer identification when required;
  - Completing AML and CTF training when required (at least annually); and
  - Being vigilant in identifying potential money laundering or terrorist financing activities.

The steps that Palmex will take to meet these responsibilities are described in staff procedural documents.

If you aren't sure what to do to meet these responsibilities, speak with your manager or the Compliance Officer.

5 Canadian AML Compliance Program Components

As a FMSB directing our services to Canadians, we are required to have in place a Compliance Program made of the elements described below. Our AML/CTF program has been designed to conform to the elements required under Canadian legislation.

5.1 Policy & Procedures

Our policy statements describe what we are required to do, while our procedures describe how we will meet these obligations. Our procedures should be detailed enough that someone could read and follow the steps described. This program document includes both policies and procedures.

All staff are required to read the Policy and Procedures for All Staff.

All staff with compliance related duties are required to read the Policy, Risk Assessment, Procedures for All Staff, and Procedures for Compliance Staff.

5.2 Risk Assessment

Our company's Risk Assessment is summarized in a separate document. It describes in detail:

- The risk that our activities could make us vulnerable to terrorist financing or money laundering and
- The controls that we have in place to prevent, detect and deter money laundering and terrorist financing[10].

The risk Assessment is reviewed and updated by the Compliance Officer at least every two years, and more often where there are changes to Canadian legislation, the products and services that we offer or our controls.

5.3 Compliance Officer

Senior Management must approve the Compliance Officer's appointment. While the Compliance Officer may or may not be a member of the Senior Management team, the Compliance Officer must always have access to management and the authority to carry out their duties. It is also vital that the Compliance Officer be educated about the ongoing compliance requirements that apply to our business. This is accomplished by attending education and training sessions, checking FINTRAC's website on a regular basis, and signing up for FINTRAC's mailing list[11].

The Compliance Officer must be accessible to all staff members who may have questions about anti-money laundering, counter terrorist financing or compliance related processes. In the case of an extended absence, a designate should be in place (and the duties of the designate should be clearly communicated to other staff members in case questions arise). For larger organizations, an assistant Compliance Officer should be appointed to act in the Compliance Officer's absence.

5.4 AML Compliance Effectiveness Review

An AML Compliance Effectiveness Review is like an audit that tests our company's AML and CTF compliance program. The review tests two elements: our program documentation (what we say we're doing) and our operations (what we've actually done during a specific period of time). These reviews must be completed at least once every two years. The results of the review are shared with Senior Management (this must be done within 30 days of the date that the final report is issued).

[10] Our controls are described at a high level in Risk Assessment documentation.
[11] https://www.fintrac-canafe.gc.ca/contact-contactez/list-liste-eng

The information gathered for these reports is very specific. If you receive a request related to a review, please check to be certain that you are able to provide all of the information that was requested. The review process may also include interviews with staff. If you are interviewed, it is fine to have a copy of our AML and CTF compliance program and other documentation with you and to refer to these during the interview.

The Compliance Officer will work to correct any issues that are noted in the report. This may include:

- Updating the AML Compliance Program;
- Creating new controls;
- Updating processes;
- Updating customer records;
- Providing additional staff training on specific topics;

The results of AML Compliance Effectiveness Reviews may also be shared with potential business partners, financial service providers and FINTRAC. It is a best practice for the Compliance Officer to keep a record of the updates that have been made based on the AML Compliance Effectiveness Review. This can be done in a simple spreadsheet.

5.5 Training & Training Plan

All Palmex staff (and any third-party contractors) are required to attend annual training. Management is required to attend bi-annual training and the compliance team attends quarterly training. Palmex encourages staff to attend external training if relevant and of interest to the employee.

New hires receive and basic AML and CTF, anti-fraud and anti-bribery training within their first 30 days on the job, as well as specific role-based training carried out by operations and compliance divisions, prior to dealing with customers or customer funds independently.

Anyone that is on a leave of absence that causes them to miss regularly scheduled training will complete training within 30 days of their return to work.

The Compliance Officer will create an annual training plan and track the completion of all training, and may require additional training sessions if compliance issues arise. A minimum score of 80% is required for any training quizzes.

AML and CTF Compliance Training will cover (at minimum) these elements:

- What is money laundering?
- What is terrorist financing?
- Who is FINTRAC?
- What is a FMSB?
- What are our responsibilities under Canadian law?
    - AML Compliance Program
        - Compliance Officer

        - AML Program
        - Risk Assessment
        - AML Compliance Effectiveness Review
        - Training
    - AML Compliance Operations
        - Reporting
        - Recordkeeping
        - Identifying Customers
        - Customer Risk
        - Transaction Monitoring
- Who is our Compliance Officer?
- What do I do if I believe that money laundering or terrorist financing is taking place?
- What indicators should I look for in our transactions and customer behaviours?

The completion of this training is mandatory (non-negotiable), and training must be completed within the time frames communicated by the Compliance Officer or their designate. Failure to complete training could expose the company to regulatory penalties. For this reason, it is vital that you contact the Compliance Officer immediately if you believe that you may not be able to complete your scheduled training session.

If you have any questions about AML and CTF compliance, please contact the Compliance Officer.

6 Operational Compliance

Operational Compliance is everything that we do in order to meet our obligations. This includes identifying our customers in some cases, reporting certain types of transactions to FINTRAC and other agencies, and keeping records.

6.1 FINTRAC Foreign MSB Registration

We must register as an FMSB with FINTRAC before conducting any transactions defined above in section 3 for any Canadian customers. The registration must be maintained, and we must:

- Keep registration information up to date;
- Respond to requests for, or to clarify, information in the prescribed form and manner, within 30 days;
- Renew our registration before it expires; and
- Let FINTRAC know if we stop offering MSB services to the public.

These requirements will be handled by the Compliance Officer or a trained delegate. As an FMSB we must also designate a representative for service in Canada. The representative we have chosen to accept, on behalf of our business, FINTRAC related notices and inquiries is Outlier Solutions Inc., which is a Canadian consulting firm, founded

in August of 2013, focused on developing compliance and AML solutions for reporting entities such as Palmex.

Our FINTRAC registration information is as follows:

- FMSB registration number: M21923040
- Initial date of registration: 2021-12-02
- Expiry date of registration:2024-08-31

6.2 Reporting

Palmex must report certain transactions to FINTRAC and other agencies as necessary. FINTRAC provides secure online forms to report these transactions. Reporting to FINTRAC should always be completed by the Compliance Officer or a designate (a person that has been trained to submit reports in the Compliance Officer's absence).

All other employees should use the internal forms included in this program to submit reports to the Compliance Officer. If you aren't sure whether or not you will need to submit a report, speak with the Compliance Officer for clarification. If it is not possible to speak with the Compliance Officer at that time, err on the side of caution by collecting the information that you need to fill out the form(s) and submit the report(s). This includes collecting the customer's identification information.

All reports have specific timelines in which they must be submitted to FINTRAC. All internal reports should be submitted to the Compliance Officer on the same day that the incident or transaction takes place.

Reports submitted by staff members are reviewed as soon as possible. Where there are issues with the reports, such as missing or incomplete information, the Compliance Officer will conduct follow up coaching sessions. The Compliance Officer will also work with the staff member to contact the customer (where possible) in order to obtain any missing or incomplete information.

The Compliance Officer will report all prescribed transactions within the required timeframes via F2R (where possible) on paper (where electronic submissions are not possible) or via FINTRAC web form where applicable.

Report Type	Applicability	Timing	Reported To	How is it submitted?
Electronic Funds Transfer Report (EFTR)	Does not apply to Palmex based on business model	5 working days from the transaction date	FINTRAC	FINTRAC Web Reporting
Large Cash Transaction Report (LCTR)	Does not apply to Palmex based on business model	15 calendar days from the transaction date	FINTRAC	FINTRAC Web Reporting

Report Type	Applicability	Timing	Reported To	How is it submitted?
Large Virtual Currency Transactions Report (LVCTR)	Applies to Palmex	5 working days after the day on which the person or entity transfers or receives the amount	FINTRAC	FINTRAC Web Reporting
Suspicious Transaction Report (STR)	Applies to Palmex	As soon as practicable from the date that a fact is discovered that causes us to have reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing	FINTRAC	FINTRAC Web Reporting
Attempted Suspicious Transaction Report (ASTR)	Applies to Palmex	As soon as practicable from the date that a fact, related to the incomplete transaction, is discovered that causes us to have reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing	FINTRAC	FINTRAC Web Reporting
Terrorist Property Report (TPR)	Applies to Palmex	Immediately	FINTRAC, RCMP, CSIS	On paper (via fax)

6.2.1 Electronic Funds Transfers (EFTs)[12]

Financial entities, money services businesses and casinos have to report incoming and outgoing international EFTs of CAD 10,000 or more in a single transaction. These include the transmission of instructions for a transfer of funds made at the request of a customer through any electronic, magnetic or optical device, telephone instrument or computer.

EFTs of CAD 10,000 or more, including two or more transactions of less than CAD 10,000 that total more than CAD 10,000 conducted by or on behalf of the same person or entity in the same 24-hour period are detected by our trade software. The 24-hour period is

[12] Palmex does not currently conduct such transactions. This has been included for education purposes only.

calculated using a static 24-hour period. An alert is generated, and the Compliance Officer resolves the alert and completes FINTRAC reporting.

Electronic funds transfers must be reported to FINTRAC within five (5) business days of the date on which the transaction takes place.

6.2.2 Large Cash Transactions[13]

Large Cash Transaction Reports (LCTRs) are submitted when a customer conducts transactions, in cash, valued at CAD 10,000 or more (in any currency or combination of currencies) in the same 24-hour period. The static 24-hour period we have chosen for calculating this is between 12:00am – 11:59pm. This may be in a single transaction or several separate transactions, including transactions conducted at different Palmex locations.

When an LCTR is required, the customer's identification must be verified, and identification information must be recorded.

A third-party determination must also be made. This means that we must ask the customer if they are completing the transaction(s) on their own behalf or someone else's. If the transactions are being completed to the benefit of someone else, we must obtain information about that person and their relationship to the person conducting the transaction.

Unlike STRs and ASTRs, it is ok to let the customer know that we must fill out an LCTR form and to fill out this form with the customer present.

LCTRs must be submitted to FINTRAC within 15 calendar days.

6.2.3 Large Virtual Currency Transactions

Large Virtual Currency Transaction Reports will have to be submitted to FINTRAC when a customer conducts transactions, in virtual currency, valued at CAD 10,000 or more in the same 24-hour period. This may be in a single transaction or several separate transactions. The static 24-hour period we have chosen for calculating this is between 12:00am – 11:59pm. This may be in a single transaction or several separate transactions.

Similar to an LCTR, we are required to verify a customer identification. We must also conduct a third-party determination. This means that we must ask the customer if they are completing the transaction(s) on their own behalf or someone else's. If the transactions are being completed to the benefit of someone else, we must obtain information about that person and their relationship to the person conducting the transaction.

[13] Palmex does not currently conduct such transactions. This has been included for education purposes only.

Large Virtual Currency Transaction Reports must be submitted to FINTRAC within 5 working days after the day on which the person or entity transfers or receives the amount.

6.2.4 Suspicious Transactions & Attempted Suspicious Transactions

Suspicious Transaction Reports (STRs) and Attempted Suspicious Transaction Reports (ASTRs) are submitted to FINTRAC where there are 'reasonable grounds' to suspect that an activity is related to money laundering or terrorist financing. These reports must be submitted whether or not the transaction or activity is completed. ASTRs are used for transactions that are not completed (whether the transaction is declined by the company or cancelled by the customer). These reports must be submitted to FINTRAC as soon as practicable after completing the measures that enabled a determination that there is reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing.

It is important not to let the customer know that we are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. We are, however, protected under Canadian law from any action when we submit a report "in good faith." In most cases, even when a case goes to court, the customer will not know that this report has been filed.

There is no monetary threshold associated with STR reporting. Therefore, reports that also meet the requirement for large cash transactions or electronic funds transfers under the PCMLTFA and Regulations should also be completed.

It is important to try to take reasonable measures to identify customers that conduct or attempt suspicious transactions. Reasonable measures may include asking the customer for photo ID. The customer may ask us why we need their identification information. In such cases, let the customer know that it is company policy to collect this information. If this information is not used for additional marketing activities, let the customer know that as well (often customers are more concerned about privacy and security issues, and reassuring them may be helpful).

6.2.5 Terrorist Property

Terrorist Property Reports (TPRs) are completed if we believe that the company may be in possession of funds or property that belong to a terrorist (either an individual or an organization).

These reports should be escalated to the Compliance Officer immediately. In some cases, property or funds must be frozen. Like STRs and ASTRs, the contents of these reports (or the fact that we are filing a report) should not be disclosed to the customer.

These reports are submitted immediately to FINTRAC as well as to the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

6.3 Responding to Law Enforcement Requests

If Palmex receives a request from law enforcement the Compliance Officer must be notified immediately. Palmex will comply with law enforcement requests, such as court orders, warrants and subpoenas that are received, so long as there is no breach of privacy legislation.

6.4 Record Keeping[14]

In order to pass a FINTRAC review or an AML Compliance Effectiveness Review, we must be able to prove that we've met our obligations. This means that there are things that will need to be recorded (either on paper or electronically). These records must be kept for at least five years (but may be kept for longer) and be in a format that can be retrieved and sorted easily.

Generally, when FINTRAC makes a request, the information must be delivered to them within 30 calendar days. Depending on the type of information request and the way that the information is stored, the Compliance Officer or a designate may need time to format and organize the information. For this reason, the following information must be stored in a format that can be retrieved and delivered to the Compliance Officer quickly:

- Certain records created in the normal course of business:
    - Records for transactions of CAD 3,000 or more (if you receive CAD 3,000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments, or if you cash CAD 3,000 or more in money orders, the name of the issuer must be on the money order);
    - Records for transactions of CAD 3,000, currency exchange transaction tickets including currency used and method of payment;
    - Records of remitting or transmitting funds of CAD 1,000 or more including currency used and method of payment;
    - Records of virtual currency transactions of CAD 1,000 or more, including the virtual currency exchange transaction ticket details:
        - The date of the transaction;
        - The name and address of the person or entity that requests the exchange;
        - The nature of their principal business or their occupation;
        - The date of birth;
        - The type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
        - The method by which the payment is made and received;
        - The exchange rates used and their source;

[14] It is understood that based on our current business model, some of the record keeping items provided below do not apply. They have been provided in the event our business model changes and for educational purposes. A full list of the records that pertain to our business are detailed in our Compliance Staff Procedure.

        - The number of every account that is affected by the transaction, the type of account and the name of each account holder;
        - Every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
        - Every transaction identifier, including the sending and receiving addresses;
    - The initiation of the sending of funds at the request of a person or entity in the amount of CAD 1,000 or more, a record of:
        - The date of the transmission;
        - The type and amount of each type of funds that is involved in the transmission;
        - The person's or entity's:
            - Name;
            - Physical address;
            - Telephone number,
            - The nature of their principal business or their occupation; and
            - In the case of a person, their date of birth.
        - The exchange rates used and their source;
        - The name and address of each beneficiary;
        - The number of every account that is affected by the transaction; and
        - Every reference number that is connected to the transaction and has a function equivalent to that of an account number.
    - The final receipt of funds at the request of a person or entity in the amount of CAS 1,000 or more, a record of:
        - The date of the remittance;
        - The date of the receipt;
        - The type and amount of each type of funds that is involved;
        - The name of the person or entity who requested the remittance;
        - Each beneficiary's:
            - Name;
            - Physical address;
            - Telephone number;
            - The nature of their principal business or their occupation; and
            - In the case of a person, their date of birth.
        - The exchange rates used for the remittance and their source;
        - if the remittance is in funds, the type and amount of each type of funds involved;
        - if the remittance is not in funds, the type of remittance and its value, if different from the amount of funds finally received;

        - The number of every account that is affected by the transaction;
        - Every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
        - The name and address of the person or entity that requested the initiation of the transaction, unless that information was not, despite the taking of reasonable measures, included with the transfer and is not otherwise known.
- Complete customer identification information;
- Complete records for Politically Exposed Persons (PEPs) and Heads of International Organizations (HIOs);
- A copy of every report sent to FINTRAC:
    - Suspicious Transaction Reports;
    - Terrorist Property Reports;
    - Large Cash Transaction Reports;
    - Large Virtual Currency Transaction Reports;
    - Electronic Funds Transfer Reports;
- Large Cash Transaction records (including a record of the third-party determination);
- Large Virtual Currency Transaction records (including a record of the third-party determination);
- Internal unusual transaction forms (whether or not they were reported to FINTRAC by the Compliance Officer) and a record of the Compliance Officer's investigation process, including a rational that describes why the transaction or attempted transaction was or was not reported to FINTRAC;
- A record of the content, date and completion/attendance of any AML or CTF related training sessions, including internal staff training sessions;
- AML Compliance Effectiveness Review reports, including a record of Senior Management sign-off on the final report;
- All FINTRAC correspondence and reporting;
- All AML and CTF compliance program documents, including policies, procedures and our Risk Assessment;
- All customer and business relationship risk ranking documentation;
- All records of enhanced due diligence for higher risk customers and business relationships;
- All records of transaction monitoring for higher risk customers and business relationships;
- Records related to business relationships; and
- Copies of signed agreements with our agents and/or service providers.

6.5 Customer Authentication & KYC

Every individual or corporate entity must undergo an onboarding process comprised of a questionnaire, customer identification as well as certain additional information such as its

planned business relationship with Palmex. Additional details on this process are outlined in our All Staff Procedure.

6.5.1 Identification Methods for Individuals

In all cases, we need to identify our customers and record specific information about the customer. This includes:

- Any customer with whom we have an ongoing service agreement;
- Virtual currency exchange transactions value at CAD 1,000 or more; and
- Large virtual currency transactions (valued at CAD 10,000 or more in a single transaction or multiple transactions within 24 hours).

And, without letting the customer know that we may have suspicions about the nature of their activities, in instances of:

- Suspected money laundering or terrorist financing activity; and
- Terrorist property.

The below chart outlines the methods that can be used to identify individuals as required by PCMLTFA and associated regulations. Details the specific processes followed in order to identify customers, as well as the additional know your customer (KYC) information collected are included in our All Staff Procedure.

Identification Method	Documents Or Information to Review	Identification Details That Must Match	Information That Must Be Recorded	Internal Notes
Government-Issued Photo Identification (Single Process)	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)	Not currently in use
Credit file (Single Process)	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 we consulted/searched the credit file Name of the credit bureau or third-party vendor Person's credit file number	Not currently in use

Identification Method	Documents Or Information to Review	Identification Details That Must Match	Information That Must Be Recorded	Internal Notes
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 financial account	Person's name Date we 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 number associated with the information if no account number exists	Currently in use
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 person's identity was verified using one of the methods in force in the PCMLTFR at that time	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	Not currently in use
Agents or Mandataries	Information in the records of the agent or mandatary for the method used Be satisfied that the information is valid and current and that the person's identity was verified by using the	The identification details listed under the identification method used	Person's name The written agreement or arrangement with the agent or mandatary for the purpose of verifying a person's identity The information provided by the agent or mandatary	Not currently in use

Identification Method	Documents Or Information to Review	Identification Details That Must Match	Information That Must Be Recorded	Internal Notes
	government-issued photo identification, credit file or dual-process methods or Where the identity was verified prior to June 1, 2021, that the person's identity was verified using one of the methods in force in the PCMLTFR at that time		that they referred to in order to verify the identity of the person	

6.5.2 Organizations[15]

When our customers, who are organizations, conduct transactions that require identification, we must collect and record the following information. Some of the information that we collect will be different depending on the type of organization being identified. For all organization types, we must collect:

- Their full legal name (no initials, short forms or abbreviations);
- The organization's structure (incorporated company, trust, partnership, etc.);
- The organization's "principal business" (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The organization's physical address (post office boxes and general delivery addresses are not acceptable for this purpose; if the customer wishes to provide a separate mailing address, we can collect this as well, but we must always record their full home address);
- The organization's telephone number; and
- Information about the organization's Directors and Beneficial Owners.

6.6 Business Relationships

We have a business relationship with anyone that has conducted two or more transactions that require identification or any customers that are entities with whom we have entered into an ongoing service agreement. For these individuals, we also need to keep a record of the nature of their business relationship with us. Although this will generally seem self-evident (for example, purchasing digital currency for personal use) it is still something that needs to be recorded.

[15] Palmex does not currently onboard clients that are organizations. This has been included for education purposes only or in the event our business model changes.

We must also conduct a Politically Exposed Foreign Person (PEFP), Politically Exposed Person (PEP), Head of an International Organization (HIO), close associate or family member of a PEP determination when we enter into a business relationship with a customer[16]. This is conducted as part of our onboarding process and periodically thereafter.

We must also conduct ongoing monitoring of our business relationships in order to:

- detect any suspicious transactions that we may need to report to FINTRAC;
- keep customer identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
- reassess the level of risk associated with our customer's transactions and activities; and
- determine whether transactions or activities are consistent with the customer information we have on hand and our risk assessment of the customer.

6.7 Risk Ranking & Transaction Monitoring

Most of our customers are considered low-risk, however, certain customers will be considered higher risk than others (medium or high-risk). This does not mean that these are "bad" people or that they have committed any crimes. High-risk customers are not treated differently when they interact with our staff, but their activities are reviewed more carefully behind the scenes.

High-risk customers are subject to regular transaction monitoring and enhanced due diligence. The Compliance Officer or a designate completes these activities. Transaction monitoring involves the review of customer transaction patterns to look for suspicious indicators. Enhanced due diligence involves additional investigation, and in some cases, the Compliance Officer may ask you to collect additional information from the customer, such as details about a specific transaction.

7 Penalties for Non-Compliance[17]

Non-compliance with Parts 1 and 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act may result in criminal or administrative penalties.

FINTRAC has legislative authority to issue an administrative monetary penalty (AMP) to reporting entities that are in non-compliance with Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its enacted regulations.

---

[16] For the remainder of our documentation, any reference to PEP and/or HIO includes all of the additional specific references and inclusions mentioned here. This has been simplified throughout our documentation to ensure clear understanding of the requirements.

[17] https://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/

FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance. Criminal penalties may include the following:

- Failure to report suspicious transactions: up to CAD 2 million and/or five years imprisonment;
- Failure to report a large cash transaction or an electronic funds transfer: up to CAD 500,000 for the first offence, CAD 1 million for subsequent offences;
- Failure to meet record keeping requirements: up to CAD 500,000 and/or five years imprisonment;
- Failure to provide assistance or provide information during compliance examination: up to CAD 500,000 and/or five years imprisonment; or
- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to two years imprisonment.

Non-criminal penalties may be issued to address repeated non-compliant behaviour. AMPs may also be used when there are significant issues of non-compliance or a high impact on FINTRAC's intelligence mandate or on the objectives of the Act and its regulations. Categories for violations where AMPs would be administered are assigned the following penalty ranges:

Categories of violations	Penalty range in CAD
Minor violation	$1 to $1,000 per violation
Serious violation	$1 to $100,000 per violation
Very serious violation	$1 to $100,000 per violation for an individual $1 to $500,000 per violation for an entity

8 Appendix: Definitions & Acronyms[18]

AML: Anti-Money Laundering

Anti-Money Laundering: actions taken to detect, deter and prevent money laundering from occurring through our business.

ASTR: Attempted Suspicious Transaction Report

Attempted Suspicious Transaction Report: a report that is filed with FINTRAC when we have reasonable grounds to suspect that a customer's activities may be related to money laundering or terrorist financing when no transaction was completed. This can include transactions that were cancelled by us, or by the customer. FINTRAC reports are filed by the Compliance Officer or designate as soon as practicable after completing the measures that enabled a determination that there is reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. If you suspect that an attempted transaction is related to money laundering or terrorist financing, you must submit an unusual transaction form to the Compliance Officer on the date that the request occurs.

Counter Terrorist Financing: actions taken to detect, deter and prevent terrorist financing from occurring through our business.

CTF: Counter Terrorist Financing

Financial Transactions and Reports Analysis Centre of Canada: Canada's financial intelligence unit and our regulator for AML and CTF. We submit reports to FINTRAC, and they have the right to examine us to test our compliance with Canadian requirements. All FINTRAC correspondences and inquiries should be passed immediately to the Compliance Officer.

FINTRAC: The Financial Transactions and Reports Analysis Centre of Canada

Large Cash Transaction: any cash transactions valued at CAD 10,000 or more that take place within the same 24-hour period for the same customer. This may include one or several transactions.

Large Cash Transaction Report: a report that is filed with FINTRAC when a large cash transaction has taken place. This report must be filed with FINTRAC within 15 calendar days of the transaction. Staff are required to report large cash transactions to the

[18] Additional definitions and acronyms can also be found here: https://github.com/ScryptoNoob/Glossary-of-Acronyms-Definitions/blob/master/AML%20and%20KYC%20Glossary.md

Compliance Officer on the day that they occur using our internal Large Cash Transaction Reporting form.

LCTR: Large Cash Transaction Report.

Large Virtual Currency Transaction Report: a report that is filed with FINTRAC when a large virtual currency transaction has taken place. This report must be filed with FINTRAC within 5 working days after the day on which the person or entity transfers or receives the amount.

LVCTR: Large Virtual Currency Transaction Report.

Money Laundering: the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Under the Criminal Code of Canada, it is illegal to launder money or to knowingly assist in laundering money. Under the PCMLTFA and Regulations, we must take steps to be sure that our business is not used to launder money and if we suspect that money laundering may be taking place, we must report it.

Money Services Business: a business that provides services in Canada: foreign exchange, remittance and/or issuing or redeeming monetary instruments. A business may also be considered a money service business in the province of Québec by providing any of the mentioned services and/or cheque cashing and/or the operation of automated teller machines.

MSB: Money Services Business.

Revenu Québec: Under the MSBA, Revenu Québec issues the licenses MSBs need to operate their businesses. They make a decision on whether to issue a license when they have received the necessary security clearance reports from the Sûreté du Québec.

STR: Suspicious Transaction Report

Suspicious Transaction Report: a report that is filed with FINTRAC when we have reasonable grounds to suspect that a transaction is related to money laundering or terrorist financing. The Compliance Officer files FINTRAC reports as soon as practicable after completing the measures that enabled a determination that there is reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. If you suspect that a transaction is related to money laundering or terrorist financing, you must submit an unusual transaction form to the Compliance Officer on the date that the transaction occurs.

Terrorism: is any attempt to influence or intimidate a government or the public at large through violent or illegal means or means that are intended to induce fear or panic.

Terrorist Financing: funding any act of terrorism or committing any act or omission that facilitates the funding of terrorism.

Terrorist Property Report: A report that is filed with several government bodies, including FINTRAC, when we believe that we may be in possession of property or funds that are owned or controlled by terrorists. The Compliance Officer files these reports immediately. If you suspect that we are in possession of terrorist property or funds, you must submit a Possible Terrorist Property Report to the Compliance Officer on the same day.

TPR: Terrorist Property Report

Unusual Transaction Report: An internal form that is used to record the details of any transactions (attempted or completed) that is suspected of being related to money laundering or terrorist financing.

UTR: Unusual Transaction Report