PALMEX GROUP INC

MONEY LAUNDERING & TERRORIST FINANCING RISK ASSESSMENT

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 Risk Assessment

PALMEX[1] is committed to preventing, detecting, and deterring money laundering and terrorist financing and has a zero-tolerance policy regarding such activities. 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. This document forms part of our anti-money laundering (AML) and counter terrorist financing (CTF) compliance program, in conjunction with our training program, policy and procedural documentation. It is also part of the enterprise-wide Risk Management Framework (RMF).

The aim of the Risk Assessment is to diagnose and document the risk that our business may be used to launder money or finance terrorism. In addition, we consider the controls that we have in place to prevent money laundering and terrorist financing, and assess the effectiveness of our controls (how well we believe we're doing). Finally, we describe the mechanism that we use to rate the risk related to each of our customers, and the controls that we put in place for higher risk customers.

Any questions or concerns about this document should be directed to the Compliance Officer.

2 Money Laundering Risk

Money Laundering is any act intended to hide the fact that funds were obtained through criminal activity. Money laundering risk is the risk that our business could be used to disguise or move criminal proceeds.

3 Terrorist Financing Risk

Terrorist Financing is funding any act of terrorism or committing any act or omission that facilitates the funding of terrorism. Terrorist financing risk is the risk that our business could be used to facilitate or disguise terrorist financing.

4 What is Considered Risk?

Risk is the likelihood of a negative occurrence or event happening and its consequences. In the context of ML/TF, risk means:

- **At the national level:** Threats and vulnerabilities presented by ML/TF that put the integrity of Canada's financial system at risk, as well as the safety and security of Canadians.

[1] Throughout our compliance documentation, "we," "our," and "Palmex" are used to refer to Palmex Limited INC

- At the Reporting Entity level: Internal and external threats and vulnerabilities that could open us up to possibility of being used to facilitate ML/TF activities.
- Threats: A person, group or object that could cause harm. In the ML/TF context, threats could be criminals, third-parties facilitating ML/TF, terrorists or terrorist groups or their funds.
- Vulnerabilities: Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities could include weak business controls or high-risk products or services.

In order for something to be attractive for money laundering or terrorist financing, certain things are generally true:

1) Value is retained over time;
2) Value can be transferred easily from one person to another (in particular across international borders); and
3) The item or asset is difficult to trace as it passes from person to person.

This is because both money laundering and terrorist financing depend on being able to separate the source of the funds from the eventual purpose. Transferring value between individuals and/or organizations often takes place in order to make tracing the assets more difficult.[2] These transfers may occur locally as well as across borders. The ideal instrument retains its value over time and can be transferred anonymously to any location.

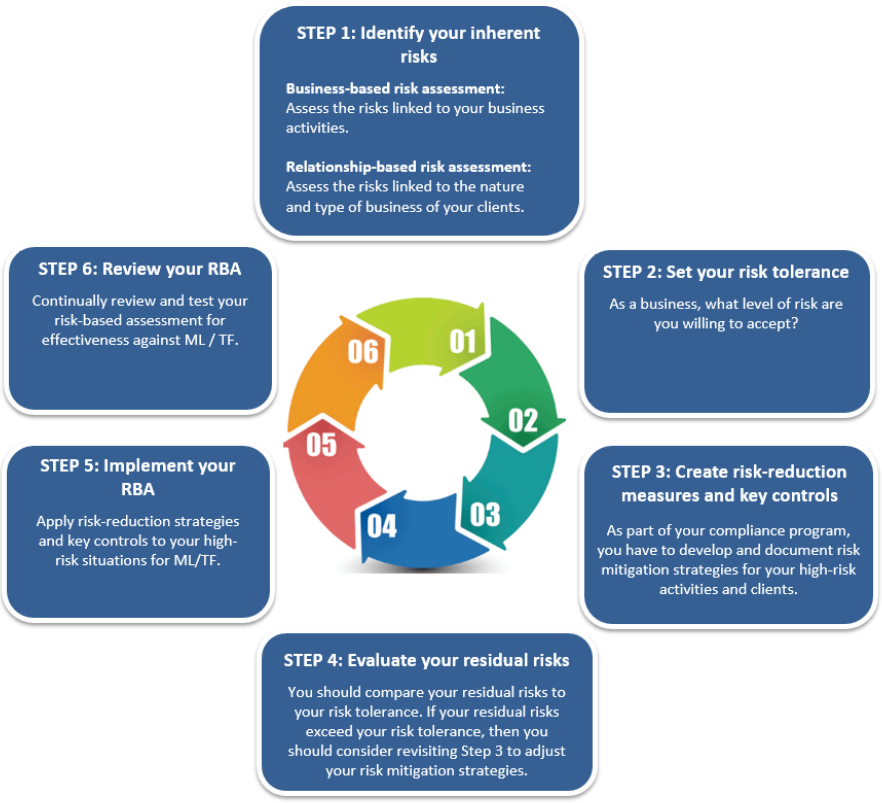
5 How Do We Assess Risk?

Although attempts to launder money, finance terrorism, or conduct other illegal activities can emanate from many different sources, certain products, services, customers, and geographic locations may be more vulnerable and have been historically abused by money launders and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as number and dollar volume, geographic location, and customers versus noncustomers, are thus be considered when PALMEX makes a risk assessment. Because of these variables, risks will vary. In formulating a risk-based approach, PALMEX identifies the significant risks and develops a risk assessment tailored to its circumstances.

We follow six steps to complete a risk assessment as per the risk-based approach (RBA) cycle depicted below. Additional information on how to conduct each step is defined throughout this document.

[2] Traditional concepts of placement, layering and integration remain critical to identification of money laundering.

Diagram 1: RBA cycle



As part of this assessment, we must consider distinct factors:

1) Products, Services and Delivery Channels: the specific goods or services that we buy and sell as well as the ways in which we serve our customers;
2) Geography: the areas in which we operate, including our suppliers, our physical locations and the areas in which our customers are located;
3) Our Customers and Business Relationships: the individuals or organizations that engage in transactional activity with our business;
4) New Developments & Technologies: changes to technology or other aspects of our business that can have a significant impact on our risk;
5) Other Factors: this includes any element of our business that is not considered in the previous categories. We consider our employees, our suppliers and our agents as additional risk factors. Specifically of focus are our recordkeeping, reporting and key operational processes that impact all aspects of our business.

Our methodology assesses the risk in each of these categories as “High-risk” “Medium-risk” and “Low-risk”. To do this, we assign a numeric score to each:

- High = 3
- Medium = 2
- Low = 1

Where a category has subcategories, the total score is obtained by taking the average risk score across all subcategories and rounded up to the nearest whole number.

An overall score of the inherent risk, for the entire business, is obtained by adding the total score across each of the five categories. The total score is ranked using the following:

- Low = 5 to 7
- Medium = 8 to 10
- High = 11+

When assessing risk, we must distinguish between inherent risk and residual risk. Inherent risk is the intrinsic risk of an event or circumstance that exists before our controls have been applied. Our inherent risk scores are largely derived from FINTRAC guidance. Residual risk is the level of risk that remains after the implementation of mitigation measures and controls have been applied. While high-risk before controls have been applied is acceptable, it is expected that our controls will reduce the risk "after controls" to Low levels in all categories. Where the risk after controls has been applied is still High, the Compliance Officer, along with Senior Management, will revise the controls.

As a business, we are willing to accept a high-risk score before controls have been applied but will not tolerate a risk score of high after controls have been applied.

6 Executive Summary

6.1 Our Business

PALMEX is a Foreign MSB under Canadian legislation. PALMEX is headquartered in Tallinn, Estonia and offers its services to Canadian customers, as well as customers in other countries around the world. 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, Ethereum and Starpoints using fiat rails such as credit card processing and other virtual currencies. PALMEX's Canadian customers reside throughout Canada (not including Québec). The vast majority of customers are expected to be repeat customers.

PALMEX is owned by Petros Kattou. The Compliance Officer is Petros Kattou.

The base of Canadian operations is from PALMEX's head office, which is located in Canada. This is an operational location; not a retail location and therefore, is not accessible by the public.

PALMEX does not carry out business in the province of Québec and therefore is not registered with the Revenu Québec. PALMEX does not use agents to conduct transactions on their behalf.

6.2 Our Risk: Business Based Risk Assessment Summary

Based on the Risk Assessment that follows, our overall money laundering and terrorist financing risk, before controls are applied, is High (3).

Our controls effectively mitigate the risks to our business; the risk that remains once our controls have been applied (our residual risk) is Low (1).

Category	Before Controls (Inherent) Risk (High/Medium/Low)	Rating (3/2/1)	After Controls (Residual) Risk (High/Medium/Low)	Rating (3/2/1)
Products, Services & Delivery Channels	High	3	Low	1
Geography	Low	1	Low	1
Customers & Business Relationships	High	3	Low	1
New Developments & Technologies	High	3	Low	1
Other Factors	High	3	Low	1
Total	High	13	Low	5

In the sections that follow, we outline the specific risks that apply to our business, the controls that we have in place to combat money laundering and terrorist financing, our mechanisms for risk ranking our customers, and the measures that are applied to our High-risk customers.

7 Our Products, Services & Delivery Channels[3]

In this section, we outline the products and services that we offer to our customers, as well as the delivery channels used to render the products and services. We also consider the methods of payment that may be used (both by our business and by our customers). Each of these has an effect on our money laundering and terrorist financing risk.

A summary of factors that are assessed under this category is as follows:

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
Services – Purchase and Sale of Virtual Currency	High	3

[3] The controls that we apply to each of these categories are discussed later, under the heading "Controls." The risk described in these sections is the risk before Palmex has applied any controls.

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
Services – Prepaid Card Services	Low	1
Payment Methods – Credit Card	Low	1
Payment Methods – Virtual Currency	High	3
Delivery Channels – Non-Face-to-Face	High	3
Total (Average)	High	3

The average money laundering and terrorist financing risk related to our products, services and delivery channels, before controls are applied, is High (3).

7.1 Products & Services

7.1.1 Purchase & Sale of Virtual Currency

Virtual currencies, such as Starpoints[4], mimic cash in that there is an exchange rate, and it can be transferred from person-to-person.

PALMEX allows for the buying and selling of virtual currency. While PALMEX conducts Know Your Customer (KYC) and identification measures for all its customers, in general, it is possible to buy, transfer and use virtual currency with some degree of anonymity (although transactional activity is captured in a public ledger, the ledger is not directly connected to the user's identity). Also, there are no set limits on the total value of virtual currency that an individual can possess or transfer.

The average transaction sizes are expected to increase and decrease with the value of virtual currencies. At present, both higher net worth individuals, businesses and investment companies appear to be entering the market, a factor that is expected to lead to price increases.

100% of our customers conduct virtual currency transactions. The average transaction value is CAD 175.

The risk of money laundering or terrorist financing through the purchase and sale of virtual currency transactions, before controls are applied, is High (3).

7.1.2 Prepaid Card Services

Open-loop gift cards, also referred to as prepaid cards, can be used to purchase goods or services. PALMEX is part of an approved Visa card issuance program based out of Singapore, which enables PALMEX's customers to apply via the App or website for a prepaid Visa card. Said cards require the customer to sell virtual assets held on the E-wallet and top up the prepaid card using the fiat proceeds. All applications for prepaid

[4] Starpoints are a stablecoin, issued by Palmex to be used within our platform.

cards require enhanced due diligence on the customer and updated KYC and AML checks when applying. These prepaid cards can only be applied for by PALMEX's Asia residing customer base and are only able to be used only in Asia, there are no plans to launch a similar offering to Canadian customers.

These cards act like cash: they are portable, valuable, exchangeable, anonymous and as a result are attractive to criminals. Generally speaking, prepaid cards can be used to launder money, and there have been a limited number of cases disclosed by FINTRAC that have involved the use of prepaid and open-loop gift cards. As a result, PALMEX restricts the ability to top up these cards (as mentioned above), runs vigorous checks when customers apply for them and monitors the use of them stringently including but not limited to rigid monthly topping up and spending limits.

It is expected that 0% of Canadian-based customers will complete transactions related to the sale of open-loop gift and or prepaid cards.

The risk of money laundering or terrorist financing through our prepaid card services, before controls are applied, is High (3).

7.2 Payment Methods

The following methods of payment are accepted from our customers and are made to our customers beneficiaries:

- Credit cards; and
- Virtual Currency.

Additional payment methods are to be added over time. New payment methods will be added to this risk assessment prior to their implementation so the associated risk is considered and adequately mitigated. An assessment of the risk related to each method of payment that we accept appears below.

Based on the average risk of accepting credit cards that we accept with regard to the risk of money laundering or terrorist financing, before controls are applied, is Low (1).

Based on the average risk of accepting virtual currencies that we accept with regards to the risk of money laundering or terrorist financing, before controls are applied, is High (3).

7.2.1 Credit Card

Acquiring a credit card requires interacting with and being identified by a financial institution. Credit card transactions over a preset threshold (set by financial institutions) require either a signature or a personal identification number to confirm the transaction. Online credit card transactions require specific information, such as the cardholder's address and a code that appears on the back of the card, and may also require a separate password to authorize the transaction.

Credit card transactions are tracked and monitored by financial institutions. Credit cards are not generally used to store value and cannot be anonymously transferred between individuals easily.

Credit card transactions account for about 95% of all payments. The average credit card transaction value is CAD 250.

The money laundering and terrorist financing risk related to credit card payments, before controls are applied, is Low (1).

7.2.2 Virtual Currency

Virtual currencies may be used to transfer value electronically, as well as to serve other functions. Although not currently captured by the Canadian definition of currency, virtual currencies mimic cash in that there is an exchange rate, and it can be transferred from user to user.

In some cases, it is possible for users to buy, transfer and use virtual currencies with some degree of anonymity (although transactional activity is generally captured in a public ledger, the ledger may not be connected to the user's identity). There are no set limits on the total value of virtual assets that an individual can possess or transfer. As virtual currencies grow in popularity and value, and marketplaces increase (creating liquidity), these assets may become more attractive to criminals.

This is particularly true where such assets may be acquired, held, traded, and sold pseudonymously.

Virtual currency transactions account for about 5% of all payments. The average virtual currency transaction value is CAD 200 for incoming payments and CAD 250 for outgoing payments.

The inherent money laundering and terrorist financing risk related to virtual currency payments, before controls are applied, is High (3).

7.3 Delivery Channels

In this section, we consider the ways our customers can access our services, and the risks based on the delivery and access channels the public has to our business.

We market our products to our Canadian customers via:

- Word of mouth (from existing customers);
- Digital marketing campaigns including but not limited to influencers;
- Web advertisement and website; and
- Social media.

Currently, we only serve our customers non-face-to-face via our website and mobile app. Email and a live chat widget on the platform are also used from a customer service perspective but not to conduct transactions.

Taken together, the risk of money laundering or terrorist financing via our delivery channels, before controls are applied, is High (3).

7.3.1 Non-Face-to-Face Transactions

PALMEX's business is solely conducted non-face-to-face through our website and mobile app. Non-face-to-face transactions allow for less interaction with our customers, which means less ability to observe typical customer behaviours that would be considered suspicious.

It is expected that 100% of business activity will be conducted non-face-to-face.

The average inherent money laundering and terrorist financing risk related to non-face-to-face delivery, before controls are applied, is High (3).

8 Geography

In this section, we consider our geographic locations as well as the locations of our customer base and suppliers. In order to do this, we consider materials published by the Financial Action Task Force (FATF)[5] and materials published by KnowYourCountry.com[6] that describe money laundering and terrorist financing risk related to particular countries.

KnowYourCountry.com numerically rates and divides country risk into these categories:

Low	Medium	High
75 - 100	50 – 74.99	<50

The FATF's publications include a list of high-risk and non-cooperative countries , i.e. countries that have not developed AML and CTF regimes or that have not made sufficient progress in developing AML and CTF regimes)[7].

Non-cooperative countries include:

- Iran; and
- Democratic People's Republic of Korea (DPRK).

We do not conduct any transactions involving non-cooperative countries, including transactions with suppliers or vendors.

[5] http://www.fatf-gafi.org/

[6] A full description of the Know Your Country methodology is included in an appendix to this document.

[7] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

We also have a list of prohibited countries that we will not allow customers to conduct transactions from, though their identification document would be considered acceptable if that is the origin (which would impact the assessment of risk related to that customer). The following countries are considered prohibited:

- Afghanistan;
- Algeria;
- Bangladesh;
- Belarus;
- Bolivia;
- Burma (Myanmar);
- Burundi;
- Cambodia;
- Central African Republic;
- China;
- Colombia;
- Democratic Republic of the Congo;
- Ecuador;
- Egypt;
- Eritrea;
- Indonesia;
- Iraq;
- Jordan;
- Kyrgyzstan;
- Lebanon;
- Libya;
- Mali;
- Mongolia;
- Morocco;
- Nepal;
- Pakistan;
- Republic of Guinea;
- Republic of Guinea-Bissau;
- Saudi Arabia;
- Somalia;
- South Korea;
- South Sudan;
- Sudan;
- Syria;
- Taiwan;
- Tunisia;
- United States of America;
- Uzbekistan;
- Venezuela;

- Vietnam;
- Yemen; and
- Zimbabwe.

Additional High-risk countries as stated by FATF include:

- Albania;
- Barbados;
- Burkina Faso;
- Cayman Islands;
- Haiti;
- Jamaica;
- Malta;
- Nicaragua;
- Panama;
- Philippines;
- Senegal;
- Turkey; and
- Uganda.

We consider the above jurisdictions to be high-risk for money laundering and terrorist financing.

While our suppliers change from time to time, we do not generally source services or suppliers from high-risk jurisdictions.

Where our customer or supplier is located in a high-risk jurisdiction, the Company ensure that appropriate controls are in place.

A summary of factors that are assessed under this category is as follows:

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
Destination & Origin of Funds – Canada	Low	1
Destination & Origin of Funds – Estonia	Low	1
Destination & Origin of Funds – United Kingdom	Medium	2
Destination & Origin of Funds – Singapore	Low	1
Location of Offices	Low	1
Customer's Locations Within Canada	Low	1
Total (Average)	Low	1

The risk of money laundering or terrorist financing related to PALMEX's geography, before controls are applied, is Low (1).

8.1 Destination & Origin of Funds

Our business is centered in Estonia and Canada, and we expect our customers and beneficiaries to be located in:

- Canada (Low-risk);
- Estonia (Low-risk); and
- Singapore (Low-risk).

As per the KnowYourCountry website the rating for each country, as well as the risk rating methodology, are included as appendices to this document. Separate sections appear below for additional analysis relating to Canada, which account for the majority of PALMEX's transactions.

The risk of money laundering or terrorist financing related to PALMEX's destination and origin of funds locations, before controls are applied, is Low (1).

8.1.1 Canada

Our customers may be located in Canada, which according to knowyourcountry.com is rated 75.72 (Not High).

Canada's most recent mutual evaluations, by the Financial Action Task Force (FATF), have been positive overall and there are currently no strategic deficiencies observed, nor sanctions against the country.

As a country, Canada is not considered a high crime area, when compared to other countries on a global scale (ranked 82nd of the 135 countries included)[8]. Additionally, when compared to other countries within the Americas (North, Central and South America), Canada is considered to have the lowest crime index (ranked 26th of the 27 countries included)[9].

It is expected that 30% of PALMEX's transactions will involve Canada.

The risk of money laundering or terrorist financing related to Canada, before controls are applied, is Low (1).

8.1.2

Customer funds may flow through , which according to knowyourcountry.com is rated 77.57/Low.

[8]https://www.numbeo.com/crime/rankings_by_country.jsp?title=2021
[9] https://www.numbeo.com/crime/rankings_by_country.jsp?title=2021&region=019

Estonia's most recent mutual evaluations by the Financial Action Task Force (FATF) have been positive overall, and there are currently no strategic deficiencies observed, nor sanctions against the country.

Estonia is considered a low-risk crime area, when analyzed on a global scale (ranked 44th out of the 137 countries included)[10]. However, when compared to other countries within Europe, Estonia is second on the scale (ranked 2nd of the 41 countries analyzed)[11], which is ranked highest crime rate to lowest.

Approximately 40% of PALMEX's transactions will involve Estonia.

The money laundering and terrorist financing risk related to Estonia, before controls are applied, is Low (1).

8.1.3 Singapore

Customer funds will flow through Singapore, which according to knowyourcountry.com is rated 76.83/Low.

Singapore's most recent mutual evaluations by the Financial Action Task Force (FATF) have been positive overall, and there are currently no strategic deficiencies observed, nor sanctions against the country.

Singapore is considered a low-risk crime area, when analyzed on a global scale (ranked 114th out of the 137 countries included)[12]. Additionally, when compared to other countries within Asia, Singapore is on the low end of the scale (ranked 32nd of the 43 countries analyzed)[13], which is ranked highest crime rate to lowest.

Approximately 5% of PALMEX's transactions will involve Singapore.

The money laundering and terrorist financing risk related to Singapore, before controls are applied, is Low (1).

8.2 Our Office Locations

PALMEX's head office is located 6th Floor - 905 West Pender Street, Vancouver, British Columbia, V6C 1L6, Canada. The current location is not known to be a high crime area[14].

Based on FINTRAC's guidance, we have developed a model to evaluate our geographic risk within Canada by considering:

- % of Total Annual Transaction Volume,
- % of All STRs Filed in the past year,

[10] https://www.numbeo.com/crime/rankings_by_country.jsp
[11] https://www.numbeo.com/crime/rankings_by_country.jsp?title=2021&region=150
[12] https://www.numbeo.com/crime/rankings_by_country.jsp
[13] https://www.numbeo.com/crime/rankings_by_country.jsp?title=2021&region=150
[14] https://www.numbeo.com/crime/in/Paris

- % of Unusual Transactions escalated to the Compliance Officer in the last year,
- % of All LCTRS Filed in the last year,
- % of All High-risk Customers and Business Relationships,
- Distance from a Border Crossing,
- Elevated crime rate,
- Rural, mid-sized, or large city,
- Near an international airport, and
- Known Issues with Staff and/or Controls.

Based on these factors, we derive and assess location risk as High, Medium or Low risk.

Location	Location Type (Office or Agent)	% of Total Annual Transaction Volume	% of All STR/ASTR Filed in the past year	% of Unusual Transactions escalated to the Compliance Officer in the last year	% of All Customers and Business Relationships Dealing with the Location	Distance from a Border Crossing in KM	The area is known to have an elevated crime rate	Known Issues with Staff and/or Controls	Other Relevant Risk Factors	Assessed Location Risk (High, Medium, Low)
6th Floor - 905 West Pender Street, Vancouver, British Columbia, V6C 1L6	Head Office	45%	0%	1%	15%	Within 150 kms	No	No	Major urban centre, close to an international airport.	Low
6th Floor - 905 West Pender Street, Vancouver, British Columbia, V6C 1L6	Office	5%	0%	0%	50%	Within 150 kms	No	No	Major urban centre, close to an international airport.	Low

Location	Location Type (Office or Agent)	% of Total Annual Transaction Volume	% of All STR/ASTR Filed in the past year	% of Unusual Transactions escalated to the Compliance Officer in the last year	% of All Customers and Business Relationships Dealing with the Location	Distance from a Border Crossing in KM	The area is known to have an elevated crime rate	Known Issues with Staff and/or Controls	Other Relevant Risk Factors	Assessed Location Risk (High, Medium, Low)
Unit 2A, 17/F, Glenealy Tower, No. 1 Glenealy, Central, Hong Kong	Office	50%	0%	0%	0%	Within 150 kms	No	No	Major urban centre, close to an international airport.	Low

The risk of money laundering and terrorist financing related to PALMEX's location, before controls are applied, is Low (1).

8.3 Our Customers' Locations Within Canada

PALMEX serves its customers via its website and mobile app. PALMEX's customers are expected to be across all of Canada (with the exception of Quebec). There does not appear to be unexpectedly dense customer groupings in areas where financial crime is known to be prevalent. However, in many cases larger urban centers do correspond to areas noted by FINTRAC as being of greater money laundering and terrorist financing concern.

The areas of highest concentration are:

- Toronto & surrounding areas;
- Montreal & surrounding areas;
- Vancouver & surrounding areas;
- South-Western Ontario (including Kitchener/Waterloo, Hamilton, and London);
- Winnipeg & surrounding areas;
- Ottawa & surrounding areas;
- Quebec & surrounding areas;
- Edmonton & surrounding areas;
- Calgary & surrounding areas;
- Regina & surrounding areas; and
- Saskatoon & surrounding areas.

The inherent money laundering and terrorist financing risk related to PALMEX's customer locations in Canada, before controls are applied, is Low (1).

9 Customers & Business Relationships

Our customers are generally individuals and businesses conducting transactions involving the jurisdictions that we service, who are looking for useability, rates and settlement superior to that offered by digital asset exchanges. We divide these customers into four categories:

- Sporadic Customers,
- Routine Customers,
- High-risk Customers, and
- Prohibited Customers.

It is expected that the majority of our customers are individuals at the onset of business.

A summary of factors that are assessed under this category is as follows:

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
Sporadic Customers & Business Relationships	Low	1
Routine Customers & Business Relationships	Low	1
High-risk Customers& Business Relationships	High	3
Prohibited Customers	High	3
Total (Average)	High	3

The risk of money laundering and terrorist financing related to our customers, before controls, is High (3).

9.1 Sporadic Customers & Business Relationships

Sporadic customers refers to customers that are new and/or expected to complete less than two (2) transactions per year. These customers generally will not have formed business relationships with us. These customers are generally considered to be low-risk.

It is expected that approximately 2.5% of our customers are considered to be sporadic customers.

These customers provide certain KYC information at onboarding and have not recently requested or completed transactions that we have reasonable grounds to believe to be related to money laundering or terrorist financing.

The inherent risk of money laundering or terrorist financing risk related to our sporadic customers, before controls are applied, is Low (1).

9.2 Routine Customers & Business Relationships

Routine customers refers to customers who conduct more than two transactions per year. These customers may or may not have formed business relationships with us. These customers are generally considered to be Medium risk.

It is expected that approximately 95% of our customers are considered to be repeat customers.

These customers provide certain KYC information at onboarding and have not recently requested or completed transactions that we have reasonable grounds to believe to be related to money laundering or terrorist financing.

The risk of money laundering or terrorist financing risk related to our routine customers, before controls are applied, is Low (1).

9.3 High-risk Customers & Business Relationships

Customers in this category may or may not have formed a business relationship with us, however, some customers may be considered high-risk without the formation of a business relationship. A list of the factors that may cause a customer to be high-risk is described under the customer risk assessment section of this document.

A very small portion of our customers (less than 3%) will be considered high-risk. Most customers deemed to be high-risk would fall into this category, as their activity has been deemed unusual due to the volume and/or velocity of their transactions. In most cases, these transactions are not considered to be suspicious, but are unusual given our business model.

The money laundering or terrorist financing risk related to our high-risk customers and business relationships, before controls are applied, is High (3).

9.4 Prohibited Customers & Business Relationships

Some customers are considered to be outside of our risk tolerance, and in these instances, we will not do business with them. This includes:

- Any person or entity believed to be a weapons, arms dealing or defence company;
- Any person or entity believed to be associated with atomic energy;
- Any person or entity believed to be dealing drugs;
- Any person or entity believed to be involved in human trafficking;
- Any person or entity believed to be involved in pornography;
- Unlicensed Gambling;
- Unlicensed fiat money service businesses (e.g., brokers, payment processors and remitters); and

- Non-licensed Bitcoin Automatic Teller Machines ("BTMs"). If the BTM is legitimately licensed, PALMEX shall determine on a case by case basis whether to maintain a relationship;
- Customers that perform transactions on behalf of third-parties;
- Any person or entity known to be involved in money laundering and/or terrorist financing related activities;
- Any person or entity believed to be attempting to use PALMEX to conduct or be paid for illegal activities; and
- Any person or entity that have been sanctioned by the U.N. and/or Canadian government.

To date, no prohibited customers and/or business relationships have been detected.

The money laundering or terrorist financing risk related to our prohibited customers and business relationships, before controls are applied, is High (3).

10 New Developments & Technologies

A summary of factors that are assessed under this category is as follows:

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
New Developments and Technologies	Medium	2
Total (Average)	Medium	2

As an existing business launching into Canada, all related technologies and compliance related recordkeeping systems relating to the new Canadian business are previously tested and known to be effective. However, there is potential for data integrity issues. As such, there is a risk of failures and/or outages but that risk is lowered based on existing implementations.

The associated risks with this category are further mitigated by the Compliance Officer being involved in the day-to-day operations of the business.

The inherent money laundering and terrorist financing risk related to new developments and technologies, before controls are applied, is Medium (2).

11 Other Factors

We have considered additional factors that may affect our money laundering and terrorist financing risk, which include:

- Relevant Operational Processes;
- Employees;
- Financial Services Suppliers (including Correspondent Banks); and

- Non-Financial Suppliers.
- A summary of factors that are assessed under this category is as follows:

Factor	Inherent Risk (High/Medium/Low)	Rating (3/2/1)
Relevant Operational Processes	High	3
Employees	High	3
Financial Services Suppliers	High	3
Non-Financial Suppliers	Low	1
Total (Average)	High	3

The average money laundering and terrorist financing risk related to our other factors, before controls are applied, is High (3).

11.1 Relevant Operational Processes

Although addressed under specific functional reviews, the AML program must also consider the overall assessment of our business' conduct with regard to record keeping, decision making responsibilities for timely and accurate regulatory reporting/supporting documentation, and key manual and automated controls.

The money laundering and terrorist financing risk related to the operations' processes, before controls are applied, is High (3).

11.2 Employees

Employees for the purpose of this risk assessment include full and part-time staff, as well as contract and seasonal / temporary staff. While all employees are expected to help us detect, deter and prevent money laundering and terrorist financing, employees are a source of risk. Employees may, knowingly or inadvertently, be co-opted by criminal groups to assist in activities related to money laundering or terrorist financing.

The PALMEX group of companies currently has 60 full-time employees, which includes an in-house developer resource. Of these employees, roughly 15 are focused on PALMEX's Canadian business.

The money laundering and terrorist financing risk related to employees, before controls are applied, is High (3).

11.3 Financial Services Suppliers (including Correspondent Banks)

Our suppliers of financial services refer to our financial institution partners, as well as correspondent banking relationships in foreign jurisdictions and exchanges where we source virtual currency from.

Like employees, suppliers may, knowingly or inadvertently, be co-opted by criminal groups to assist in activities related to money laundering or terrorist financing. Suppliers of financial services are desirable by criminals, since they provide a direct avenue to place illicit funds into the legitimate economy, as well as disguise relatively large sums of money moving on an international scale.

The money laundering or terrorist financing risk related to our suppliers of financial services, including our correspondent banking relationships, before controls are applied, is High (3).

11.4 Non-Financial Suppliers

Our suppliers of non-financial services include IT service providers, consultants, and lawyers. Like employees, our suppliers of non-financial services may, knowingly or inadvertently, be co-opted by criminal groups to assist in activities related to money laundering or terrorist financing.

While these types of relationships do not directly relate to dealing with customer funds, there is risk related to the access of a customer's private information, such as banking and identification details.

The money laundering or terrorist financing risk related to our suppliers of non-financial services, before controls are applied, is Low (1).

12 Controls

We take our duty to prevent, detect, and deter money laundering and terrorist financing seriously, and have developed controls to ensure that our business is not used to launder money or finance terrorism. The controls listed below include primary controls (designed specifically for AML and CTF purposes) and secondary controls (controls designed for other purposes that also help us fight money laundering and terrorist financing). The controls described in this section are general and apply to PALMEX's business as a whole. Specific regional processes are described in the Compliance Procedures for each region in which we operate.

13 Products, Services & Delivery Channels Controls

13.1 Products, Services & Delivery Channel Controls – General

- All of our facilities have security systems in place, which includes secure entry to restricted areas (by key or card) to prevent unauthorized or anonymous access.
- All of our facilities have security systems in place, which includes video surveillance to prevent unauthorized or anonymous access.
- All of our facilities have security systems in place, which includes alarm systems to prevent unauthorized or anonymous access.

- All of our IT-related devices and data access points have security systems in place, which includes secure access, authentication and monitoring to prevent unauthorized or anonymous access.
- Access to any AML or CTF related reports that is restricted to the Compliance Officer and designates.

The residual risk (after controls have been applied) is Low (1).

13.2 Products & Services Controls – General

- PALMEX does not conduct transactions that involve countries listed as non-cooperative with the FATF.
- If we conduct any transactions that involve jurisdictions listed as high-risk by the FATF, they are subject to additional controls, which may include verification related controls and jurisdiction specific transaction thresholds[15].
- Transaction limits apply to each transaction. Our transaction limits are stipulated in section 20.
- Staff are trained to ask additional questions if the transaction a customer is requesting doesn't make sense.
- All staff members are trained to recognize suspicious transactions/customer behaviour and ask additional information.
- If there is any doubt about the information and/or identification that a customer provides, additional documentation will be requested.
- Staff are trained to ask additional questions if the transaction that a customer is requesting doesn't make sense.
- The Compliance Officer or delegate conducts transaction monitoring.
- All transactions that we process are entered into our electronic recordkeeping system. We do not conduct "off the record" transactions under any circumstances.
- Records of all customer transactions are maintained electronically in our transaction software.
- Specific transaction limits as stipulated in section 20 and thresholds are housed in PALMEX's IT systems.

The residual risk (after controls have been applied) is Low (1).

13.2.1 Purchase & Sales of Virtual Currency Controls

- We only enable customers to redeem virtual currencies that we believe are reputable, secure and have the potential for long term growth.
- We do not support any virtual currencies that we believe to be developed for the purpose of criminal activity.

[15] In some cases, Palmex, based on Palmex's risk tolerance, establishes thresholds. In other instances, thresholds are based on jurisdictional transaction limits established by local governments or banking service providers.

- We do not support with any virtual currencies that we believe are controlled by criminals or criminal groups.
- Significant research is conducted before new virtual currencies are added to the platform.

The residual risk (after controls have been applied) is Low (1).

13.2.2 Prepaid Card Services Controls

- We only deal with the gift cards from companies that we have vetted and are reputable. Specifically, Visa and Mastercard.
- Ergo, we do not deal in any gift cards that we believe to be developed for the purpose of criminal activity.
- We do not deal with any gift cards that we believe are controlled by criminals or criminal groups.
- There are transaction limits in place which limit each customer to a single gift card per transaction.
- Reloading of the card is not permitted using virtual assets only fiat via the platform.
- Canadian customers will not be given access to apply for and or use prepaid cards issued by PALMEX.

The residual risk (after controls have been applied) is Low (1).

13.3 Payment Methods Controls - General

- If we suspect that a transaction is being conducted for the benefit of someone other than our customer, additional information/documentation is requested, and the transaction may be rejected at the Compliance Officer's discretion.

Additional controls and residual risk ratings for each subcategory appear below.

After the application of controls, the residual risk for this category is Low (1).

13.3.1 Credit Card Controls

- All credit card payments are subject to transactions limits as stipulated in section 20.
- Card payments are accepted only from the individual that owns the card.
- All credit card transactions require a form of authentication information to complete.
- Where credit card authentication fails, the transaction cannot be completed.
- If there is doubt about the card's ownership, identification documents may be requested.
- All credit card transactions are checked by 2 independent fraud platforms that risk score the transaction before authorizing it.

The residual risk (after controls have been applied) is Low (1).

13.3.2 Virtual Currency Payment Controls

- We only deal in virtual currencies that we believe are reputable, secure and have the potential for long term growth.
- We do not deal in any virtual currencies that we believe to be developed for the purpose of criminal activity.
- We do not deal with any virtual currencies that we believe are controlled by criminals or criminal groups.
- Significant research is conducted before new virtual currencies are added to the platform.
- All virtual currency payments in and out of the wallet are checked by Chainalysis, a market leading platform that allows us to check that the counter-party wallets have not been involved in any prohibited transactions in the past.

The residual risk (after controls have been applied) is Low (1)

13.4 Delivery Channels Controls – General

- Transaction monitoring, KYC check, and list screening are conducted.
- All staff that interact with customers receive AML and CTF training, including training related to suspicious indicators.
- All staff is encouraged to notify the Compliance Officer if a customer's request is unusual or suspicious.
- The Compliance Officer is involved in the day-to-day business, and aware of any new delivery channel implementations well in advance.

The residual risk (after controls have been applied) is Low (1).

13.4.1 Non-Face-to-Face Controls

- PALMEX will build profiles for customers and will actively monitor for behaviour that does not fit the customer's profile.
- The identification on file must be up-to-date for all transactions.

The residual risk (after controls have been applied) is Low (1).

14 Geography Controls - General

- PALMEX does not conduct transactions that involve countries listed as non-cooperative by the FATF.
- If we conduct any transactions with countries included in the UN Security Council Sanctions Lists, additional processes and approvals are required.
- If we conduct any transactions that involve jurisdictions listed as high-risk by the FATF, that are subject to additional controls, which may include verification related controls and specific transaction thresholds.

The residual risk (after controls have been applied) is Low (1).

14.1 Destination & Origin of Funds Controls

- Where we are aware through authoritative sources and/or adverse media that an area in which our customers are located may be a high intensity financial crime area, or may be subject to particular types of financial crime, the Compliance Officer will consider the implementation of additional controls.
- Each customer's location is considered as part of the customer's risk ranking and risk profile, which is updated on a regular basis.
- Our Compliance Officer monitors relevant information pertaining to our customer's locations within Canada on a regular basis.
- If we suspect that a transaction is related to a prohibited jurisdiction, we may suspend or prohibit the customer that initiated the activity.
- Countries that are deemed to be high-risk but are within PALMEX's risk tolerance may require enhanced due diligence.
- Transactions to or from countries deemed to be high-risk require additional review before the transaction is completed.

The residual risk (after controls have been applied) is Low (1).

14.1.1 Canada Controls

- All customers are identified before they can complete a transaction.
- All staff members are trained to recognize suspicious activity and ask additional probing questions.
- High risk customer spending is limited to CAD 2,000 in a 24-hour period,
- High risk customer spending is limited to CAD 5,000 in a 7 day period, or
- High risk customer pending is limited to CAD 7,500 in a 30 day period.

The residual risk (after controls have been applied) is Low (1).

14.1.2 Estonia Controls

- All customers are identified before they can complete a transaction.
- PALMEX staff are located in this country and are therefore intimately familiar with typical customer patterns and behaviour.
- All staff members are trained to recognize suspicious activity and ask additional probing questions.

The residual risk (after controls have been applied) is Low (1).

14.1.3 Singapore Controls

- All customers are identified before they can complete a transaction.
- PALMEX staff are located in this country and are therefore intimately familiar with typical customer patterns and behaviour.
- All staff members are trained to recognize suspicious activity and ask additional probing questions.

The residual risk (after controls have been applied) is Low (1).

14.2 Our Office Locations Controls

- Access to any AML or CTF related reports is restricted to the Compliance Officer and delegates (where applicable).
- Access to our electronic records systems is restricted to staff members that have a legitimate reason to use those systems.
- We have in place firewalls, encryption and other security measures to ensure that our information is not accessed without authorization.
- We do not locate our offices in areas that we believe to be areas of concern related to financial crime, including money laundering, terrorist financing or fraud related crimes.
- PALMEX does not operate locations in jurisdictions that have been deemed to be non-cooperative by the FATF.

The residual risk (after controls have been applied) is Low (1).

14.3 Our Customer Locations Controls

- Each customer's location is considered as part of the customer's risk ranking and risk profile, which is updated on a regular basis.
- Our Compliance Officer monitors relevant information pertaining to our customer's locations within Canada on a regular basis.
- If there are reasonable grounds to suspect that a transaction may be related to money laundering or terrorist financing, we may suspend or prohibit the customer that initiated the activity and submit an ASTR/STR.

The residual risk (after controls have been applied) is Low (1).

15 Customers & Business Relationships Controls

- All customers and business relationships are required to complete full KYC process.
- All customers and business relationships are subject to transaction monitoring, and in the case of business relationships, the nature and purpose of the business relationship is considered.
- All customers and beneficiaries are screened against publicly available lists.
- Records of all customer transactions are maintained electronically. All transactions that we process are entered into our recordkeeping system. We do not conduct "off the record" transactions under any circumstances.

The residual risk (after controls have been applied) is Low (1).

15.1 Sporadic Customer & Business Relationships Controls

- Customer due diligence (CDD) and transaction monitoring are applied to all customers (regardless of whether or not a business relationship has been formed).
- Know Your Customer (KYC) information is collected for all customers.

The residual risk (after controls have been applied) is Low (1).

15.2 Routine Customer & Business Relationships Controls

- Customer due diligence (CDD) and transaction monitoring are applied to all customers (regardless of whether or not a business relationship has been formed).
- Know Your Customer (KYC) information is collected for all customers.
- More data is available at the time of monitoring which provides additional understanding of what is expected for the customer and their transactions.
- Where a business relationship is formed, the purpose and intended nature of the business relationship is recorded.

The residual risk (after controls have been applied) is Low (1).

15.3 High-risk Customer & Business Relationship Controls

- All measures that are applied to sporadic and routine customers and business relationships are applied.
- Enhanced transaction monitoring is conducted for all high-risk customers and business relationships.
- Enhanced due diligence (EDD) is conducted for all high-risk customers and business relationships. The EDD activities are tailored to mitigate the ML and/or TF risk factors that lead to the assessment of the customer as high-risk.
- At the discretion of the Compliance Officer, any customer or business relationship may be considered high-risk.
- Where beneficial ownership cannot be confirmed, a customer that is an entity will be considered high-risk.
- If there is any doubt about the identification documents or other documents that a customer provides, additional documents will be requested.

The residual risk (after controls have been applied) is Low (1).

15.4 Prohibited Customer Controls

- All potential customers are screened against terrorist watchlists, sanctions lists, and our internal blacklist (which includes customers that are outside of our risk tolerance for a variety of reasons).
- Prohibited customers are prevented from conducting any additional transactions.
- All customers residing in prohibited countries are prevented from conducting any transactions.

The residual risk (after controls have been applied) is Low (1).

16 New Developments & Technologies Controls

- The Compliance Officer is involved in the day-to-day business, and aware of any new development and/or technology implementations well in advance.

- The Compliance Officer stays up-to-date on the Canadian regulatory landscape and attends training that has a Canadian regulatory aspect.
- All new systems are thoroughly tested before implementation.

The residual risk (after controls have been applied) is Low (1).

17 Other Factor Controls

- The Compliance Officer is directly involved in the business, and aware of any relevant changes that may require the implementation of additional controls.
- PALMEX has in place a security policy.

The residual risk (after controls have been applied) is Low (1).

17.1 Relevant Operational Process Controls

- PALMEX's AML Compliance program is the subject of external review occurring at least every two years, and more frequently where required by local regulation or banking service providers.
- Transactions may be subject to additional quality assurance measures.
- PALMEX's Compliance Officer is a member of Senior Management.
- The Compliance Officer is involved in the day-to-day business, and aware of any new operational process implementations well in advance.

The residual risk (after controls have been applied) is Low (1).

17.2 Employee Controls

These controls ensure that the staff that we hire (including part-time and seasonal staff) cannot be easily co-opted by money launderers or terrorists.

- All staff receive AML and CTF training within 30 days of beginning employment, and at least annually while they are part of our staff.
- All staff have easy access to our AML and CTF program including internal reporting forms.
- All staff are trained and expected to submit reports to the Compliance Officer where there is any suspicion of money laundering or terrorist financing.
- We screen all new staff using a process that includes interviews and reference checks. Criminal background checks may also be conducted depending on the position and jurisdiction of the individual.
- Staff turnover is not high and when there is staff turnover consideration is given to why the employee left and how this will impact maintaining AML and CTF controls and processes.

The residual risk (after controls have been applied) is Low (1).

17.3 Financial Services Supplier (including Correspondent Banks) Controls

- We only deal with reputable suppliers that we know either by association within the industry or verifying (for example by searching online) the supplier's reputation.
- We do not deal with suppliers that are located in countries listed as non-cooperative by the FATF.
- If we deal with a supplier in a country that is listed as high-risk by the FATF, the Compliance Officer is consulted on the decision before any agreements are signed.
- We will not deal with suppliers that we know have been associated with money laundering or terrorist financing activity.
- We only deal with financial services suppliers that we believe have effective AML and CTF controls in place.

The residual risk (after controls have been applied) is Low (1).

17.4 Non-Financial Supplier Controls

- We only deal with reputable suppliers that we know either by association within the industry or verifying (for example by searching online) the supplier's reputation.
- We do not deal with suppliers that are located in countries listed as non-cooperative by the FATF.
- If we deal with a supplier in a country that is listed as high-risk by the FATF, the Compliance Officer is consulted on the decision before any agreements are signed.
- We will not deal with suppliers that we know have been associated with money laundering or terrorist financing activity.

The residual risk (after controls have been applied) is Low (1).

18 Relationship-Based Risk Assessment: Customer & Business Relationship Risk Ranking

Certain customers may pose a higher risk of money laundering and/or terrorist financing with respect to unique characteristics, such as: the type of customer, their occupation (for individuals), how often they transact and the duration of the relationship with the business. We divide our customers and business relationships into High, Medium, and Low risk buckets based on their activities.

High-risk customers are flagged in our IT platform directly in the customer's profile, which changes over time based on the parameters that are detailed in our IT system. At a high level, risk parameters that are considered are as follows:

- The risk posed by the combination of products, services and delivery channels the customer uses. This is determined by looking at factors of services used and monthly volumes comparisons.
- The risk posed by the geographical location of the customer and their transactions. This is determined by looking at such factors such as the address on record and physical location of transactions.
- The risk posed by the customer's characteristics, this is determined by looking at factors such as residency, industry/occupation risk, customer income compared to transaction activity/volume, STR volume, and length of the relationship.
- We also consider the risks related to:
    - Jurisdiction of the customer,
    - Product purchases,
    - Type of customer,
    - Transaction type,
    - Transaction volume,
    - Transaction frequency,
    - Technology for example mobile, desktop IP addresses consistent with customer habits, and
    - Transaction channel.

The Compliance Officer is responsible for determining and updating customer risk ranking parameters.

In addition, the Compliance Officer is able to manually adjust risk ratings, based on activity that may not be captured in the system. In all instances, where a risk rating has been manually adjusted, detailed notes are added to the IT system explaining the rationale for the adjustment, and will be maintained for a period of five years.

18.1 Business Relationships

We have a business relationship with any customer that has completed two or more transactions that require the customer to be identified. For clarity, this can be done in a single transaction where two triggering events occur.

In these cases, we must collect and record information about the "purpose and nature" of that business relationship.

Where we are conducting enhanced due diligence, including enhanced transaction monitoring, for higher risk customers and/or business relationships, we will compare the customer's activities to the stated nature and purpose of the business relationship.

We also conduct a Politically Exposed Person (PEP) or Head of an International Organization (HIO) determination when we enter a business relationship with a customer. Currently it is our practice to complete this at onboarding and periodically throughout the relationship with the customer.

18.2 Customers & Business Relationships That Are Medium & Low Risk

Most of our customers that do not form business relationships will not be high-risk.

These will be customers who are conducting transactions that appear to be within their means (the transaction makes sense for the customer) and do not appear to have any relation to money laundering or terrorist financing.

Unless there is a reason to consider these customers and business relationships to be higher risk, customer and business relationship risk is rated as low-risk.

Where the threshold for high-risk or prohibited risk is met, a customer is moved to this category (whether or not they have formed a business relationship with PALMEX).

In rare instances, a customer or business relationship may be moved out of the High or prohibited risk categories and placed in the Medium risk category. These may include cases of mistaken identity (where a person was believed to be a blacklisted individual, but is not), or instances where additional information about the customer and their transactions becomes available later on and mitigates the risk that they were believed to pose to PALMEX. In such cases, a detailed rationale must be documented.

18.3 High-risk Customers & Business Relationships

When we define customers as High-risk, it does not indicate that we believe that our customers are criminals or involved in money laundering or terrorist financing activities. We are merely acknowledging that based on what we know about the customer and their transactions, they pose a greater risk.

For our business, the following customers are always deemed to be high-risk:

- PALMEX is aware that the customer is under investigation by a regulator;
- For non-individual customers, those for whom a beneficial ownership determination has not been completed or for whom beneficial ownership information has not been confirmed;
- Individual customer's occupation is identified as one of the following which can be classified as "gatekeepers": (Accountant, Financial Advisor, Financial Planner, Investment Analyst, Investment Banker, Lawyer, Real Estate Broker or Agent); and
- Non-individual customers whose line of business is considered vulnerable to ML/TF as a result of being a cash intensive business including the following categories: Money Services Businesses, Pawn Shops, Jewellery Stores, Restaurants, Hotels, Convenience Stores, Privately owned automated teller machines (ATMs), Vending machine operators, Parking garages.
- Customers that have triggered a suspicious transaction report or attempted suspicious transaction report within the past year;
- Customers that have triggered 3 or more suspicious transaction reports and/or attempted suspicious transaction reports within the span of our relationship with the customer;

- Customers that appear to have ongoing financial ties with a FATF non-cooperative jurisdiction;
- Customers that, where identification was required and requested, have consistently refused to be identified, including customers that have altered a transaction request in order to avoid customer identification requirements;
- Politically exposed persons (such as politicians, diplomats and their immediate families) where we are aware that the individual is politically exposed;
- Customers that perform transactions on behalf of third-parties but are unwilling or unable to provide complete details about the third-parties; and
- Customers that are organizations that seem to be deliberately structured in a way that makes it difficult to determine who owns or controls the organization.
- Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions.

The Compliance Officer maintains knowledge of High-risk customers. A sample High-risk customer log can be found in an appendix to this document. This appendix is included as a sample only; customer risk rankings and notes on compliance related activities for actual customers are housed in our IT systems.

We consider some customers to be too high-risk. In these instances, we may know, rather than suspect that the customer is involved in criminal activity. In these instances, additional IT-based controls will be applied to prevent the customer from accessing our products and services.

18.4 Prohibited Customers & Business Relationships

We may consider some customers to be too high-risk. In these instances, we may know, rather than suspect that the customer is involved in criminal activity. This includes:

- Any person or entity believed to be a weapons, arms dealing or defense company;
- Any person or entity believed to be associated with atomic energy;
- Any person or entity believed to be dealing drugs;
- Any person or entity believed to be involved in human trafficking;
- Any person or entity believed to be involved in pornography;
- Unlicensed Gambling;
- Unlicensed fiat money service businesses (e.g., brokers, payment processors and remitters); and
- Non-licensed Bitcoin Automatic Teller Machines (“BTMs”). If the BTM is legitimately licensed, PALMEX shall determine on a case by case basis whether to maintain a relationship;
- Customers that perform transactions on behalf of third-parties;
- Any person or entity known to be involved in money laundering and/or terrorist financing related activities;
- Any person or entity believed to be attempting to use PALMEX to conduct or be paid for illegal activities; and
- Any person or entity that have been sanctioned by the U.N. and/or Canadian government.

In these instances, our IT platform will automatically refuse any attempts by these customers to conduct transactions.

19 Transaction Monitoring & Enhanced Transaction Monitoring

The Compliance Officer or a designate, monitors transactions for potentially suspicious transactions. All other staff will also escalate unusual transactions to the Compliance Officer.

For High-risk customers and business relationships, enhanced transaction monitoring is conducted. The Compliance Officer reviews the information that is on file about the customer, as well as records of the customer's activity for the past two years. If there is activity that appears to be related to money laundering or terrorist financing, appropriate reports are filed with the appropriate authorities: FINTRAC (and in the case of terrorist property, with CSIS and the RCMP).

High-risk customer accounts are reviewed at least every 6 months, and more frequently where triggered by customer activity (for example, where there is an internal report submitted to the Compliance Officer).

All notes about compliance related activities for our customers are housed in our IT systems. The Compliance Officer will maintain complete records of the reviews and maintain these records for at least five years.

20 Enhanced Due Diligence

High-risk customers require a level of due diligence beyond what we do for regular customers. For this reason, when the Compliance Officer or designate performs transaction monitoring for high-risk customers, they may also conduct an internet search for additional information about the customer.

Any results that are related to criminal activity or that indicate that the customer has provided false or misleading information will be noted in the log. At the discretion of the Compliance Officer, appropriate reports are filed, as necessary, with FINTRAC (and in the case of terrorist property, with the Canadian Security Intelligence Service (CSIS)[16] and the Royal Canadian Mounted Police (RCMP)[17]).

Additional enhanced due diligence activities may apply according to the customer's high risk profile (the reason that the customer is considered to be high-risk). For example, if there was doubt regarding the veracity of any KYC information provided by the customer, documentation substantiating the customer's claim would be requested. Some examples of the EDD that may be performed incudes:

[16] https://www.canada.ca/en/security-intelligence-service.html
[17] http://www.rcmp-grc.gc.ca/en/home

- IP address doesn't match that of the credit card address,
- The user's IP address is different to the users previous last 5 transactions,
- Larger transactions than normal for that user,
- Frequency of transactions increases (during unusual times, we expect increases in users spending when there are professional and amateur Esports tournaments taking place):
    - Change in redemption patterns,
    - Using more than 5 credit cards in a 30 day period,
    - Contacting customer service to change their registered email address,
    - Any other customers/partners determined by PALMEX to be classified High-risk,
    - Where a product or transaction is considered by its nature to be higher risk, or
    - In any case where the relevant person discovers that a customer has provided false or stolen identification documentation or information PALMEX suspend the account.
- EDD will implement financial transaction thresholds, and EDD must be applied once the threshold has been breached. The thresholds will be decided on a risk-based approach and therefore will vary. Any changes to the thresholds set out below must be agreed in writing and signed off by the Compliance Officer and senior management.
    - Spending CAD 2,000 in a 24-hour period,
    - Spending CAD 5,000 in a 7 day period, or
    - Spending CAD 7,500 in a 30 day period.
- PALMEX notes that the default guideline, states that EDD must be completed in any one of the following circumstances:
    - a customer transacts over CAD 10,000 in a 12-month period
    - a customer completes more than 10 transactions per day, regardless of value

21 Updates to Customer Information & Identification

All active customers[18] subject to our Customer Due Diligence (CDD)/Know Your Customer (KYC) processes are reviewed on a periodic basis. The review may trigger updates to their information on file.

These periodic reviews include analysis of the customer's identification documentation, previous 12 months of transaction history and, where possible, any results from the Google searches conducted by the Compliance Officer. These reviews are conducted on the following schedule, based on the customer's risk rating:

- High-Risk – daily to every 6 months;

[18] Active customer means any customer that has conducted a transaction within the past year.

- Medium-Risk – 9 months; and
- Low-Risk – at least every 12 months.

Reviews of customer files may also be triggered by expired identification documents, or, where the Compliance Officer has become aware of factors that would affect the customer's risk rating, both positively and negatively.

Any requests for change, related to a customer's risk rating, must be approved by the Compliance Officer, or a delegate, regardless of the adjustment being requested.

It is at the sole discretion of the Compliance Officer whether or not additional information is required in order to make the update. All instances related to changing the risk rating of a customer will be recorded and maintained by the Compliance Officer. These records will include the rationale for the change.

22 Appendix: Compliance Officer References

In order to keep our Risk Assessment up to date, the Compliance Officer will use these references:

22.1 Financial Action Task Force (FATF)

www.fatf-gafi.org/

The FATF publishes lists of countries that are non-cooperative and high-risk. There are also detailed evaluations of member countries, including Canada and the United States.

Most AML and CTF legislation is based on the FATF's recommendations (also published on their website).

22.2 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

www.fintrac-canafe.gc.ca

FINTRAC's site links to Canadian AML and CTF legislation, as well as providing guidance to reporting entities and free training materials. There is also a mailing list for those who wish to receive news about new developments.

22.3 Know Your Country

http://knowyourcountry.com/

This site is a resource that combines various country risk metrics into a single numerical rating with a consistent methodology. The site is privately maintained.

22.4 Office of the Superintendent of Financial Institutions (OSFI)

www.osfi-bsif.gc.ca

Although the guidelines that OSFI publishes do not apply to dealers in money services business, it can be useful as best practice, in particular for larger organizations. OSFI's Guideline B-8 deals specifically with AML and CTF program development.

23 Appendix: Sample High-risk Customer & Business Relationship Monitoring & Due Diligence Log

The Compliance Officer or a designate will use this log to maintain a list of the transaction monitoring and due diligence that has taken place for high-risk customers and business relationships.

All logs (including customers that are no longer designated as high-risk) will be maintained for at least five years.

Customer Name / Identifier	Business Relationship (Yes/No)	Nature & Purpose of Business Relationship	High-risk (Yes/No)	High-risk Reason	Monitoring Date	Notes	Enhanced Monitoring Date (High-risk Only)	Notes	Enhanced Due Diligence Date (High-risk Only)	Notes	Next Follow Up (Must be within 2 years for all business relationships and one year if the customer is high-risk)	Additional Compliance Officer Notes

24 Appendix: Country Risk Rating Methodology

The KnowYourCountry.com risk-ranking tool has been designed to provide a measure of the money laundering and terrorist financing risk of countries that we might have customer relationships with and/or doing business with.

Based upon data collected from many international and government agencies, KnowYourCountry.com has subjectively weighted the findings to provide a free rating tool that is predominantly focused on money laundering and sanctions issues. Please see below our weightings and a list of all data subject sources.

	Indicator/Sub Indicator	Weighting
1	Money laundering/terrorist financing risks	56
	1.1 FATF Uncooperative/AML Deficient	25
	1.2 FATF Compliance	10
	1.3 US State ML Assessment	15
	1.5 US Secretary of State terrorism	6
2	International sanctions	15
3	Corruption risks	10
4	World Governance Indicators	3
5	Narcotics Major List	3
6	Human Trafficking	3
7	EU Tax Blacklist	5
8	Offshore Finance Centre	5

25 Appendix: Country Risk Table[19]

Last updated: October 22, 2021

Low	Medium	High
75 - 100	50 – 74.99	<50

Rank.	Country	Score
1	Sweden	**87.56**
2	Åland Islands	**86.76**
3	Finland	**86.76**
4	Norway	**86.59**
5	Svalbard and Mayen	**86.59**
6	New Zealand	**86.17**
7	Tokelau	**86.17**
8	Denmark	**85.92**
9	Faroe islands	**85.92**
10	Iceland	**85.22**
11	Greenland	**85.03**
12	Estonia	**84.35**
13	Slovenia	**84.23**
14	San Marino	**83.91**
15	Lithuania	**83.51**
16	Bermuda	**83.4**
17	Andorra	**82.39**
18	Namibia	**81.19**
19	Brunei Darussalam	**81.06**
20	Vatican City State (Holy See)	**80.42**
21	Oman	**80.41**
22	Croatia	**80.05**
23	Austria	**79.97**

[19] https://www.knowyourcountry.com/country-ratings-table

Rank.	Country	Score
24	Australia	**79.72**
25	Christmas Island	**79.72**
26	Cocos (Keeling) Islands	**79.72**
27	Norfolk Island	**79.72**
28	Puerto Rico	**79.04**
29	American Samoa	**78.84**
30	Mongolia	**78.18**
31	Chile	**78.13**
32	Guam	**78**
33	South Korea	**77.94**
34	Germany	**77.82**
35	Fiji	**77.77**
36	Japan	**77.74**
37	France	**77.69**
38	French Polynesia	**77.69**
39	Guadeloupe	**77.69**
40	Mayotte	**77.69**
41	New Caledonia	**77.69**
42	Saint Berthélemy	**77.69**
43	Saint Martin (French part)	**77.69**
44	Saint Pierre and Miquelon	**77.69**
45	Wallis and Futuna	**77.69**
46	Bhutan	**77.68**
47	French Guiana	**77.67**
48	Martinique	**77.62**
49	Anguilla	**77.57**
50	Montserrat	**77.55**
51	Réunion	**77.54**
52	Portugal	**77.52**

Rank.	Country	Score
53	Sri Lanka	**77.34**
54	Switzerland	**77.13**
55	Rwanda	**77.09**
56	Malawi	**76.87**
57	Ethiopia	**76.87**
58	United States Virgin Islands	**76.84**
59	Singapore	**76.83**
60	Solomon Islands	**76.76**
61	Czech Republic	**76.51**
62	Zambia	**76.5**
63	Guernsey	**76.44**
64	Latvia	**76.11**
65	Belgium	**76.01**
66	Canada	**75.72**
67	Greece	**75.61**
68	Uruguay	**75.55**
69	Niue	**75.52**
70	Liechtenstein	**75.42**
71	Ireland	**75.42**
72	Jersey	**75.34**
73	Spain	**75.33**
74	Tonga	**75.2**
75	Saudi Arabia	**75.15**
76	Mauritania	**75.13**
77	Isle Of Man	**75.11**
78	Macedonia, North	**75.07**
79	Poland	**74.89**
80	Luxembourg	**74.82**
81	Gambia	**74.76**

Rank.	Country	Score
82	Taiwan	**74.72**
83	North Mariana Islands	**74.64**
84	United States	**74.64**
85	Lesotho	**74.61**
86	British Indian Ocean Territory	**74.38**
87	Falkland Islands (Malvinas)	**74.38**
88	Pitcairn	**74.38**
89	Saint Helena, Ascension and Trista	**74.38**
90	United Kingdom	**74.38**
91	Slovakia	**74.15**
92	Hungary	**74.03**
93	Maldives	**74.02**
94	Macau	**73.75**
95	Niger	**73.26**
96	Marshall Islands	**73.24**
97	Micronesia	**73.12**
98	Madagascar	**73.04**
99	Bulgaria	**73.03**
100	Nauru	**72.83**
101	Togo	**72.78**
102	Nepal	**72.66**
103	Swaziland (Eswatini)	**72.62**
104	Cook Islands	**72.6**
105	Kuwait	**72.57**
106	Qatar	**72.53**
107	Italy	**72.41**
108	Botswana	**72.38**
109	Gabon	**72.32**
110	Gibraltar	**72.02**

Rank.	Country	Score
111	Papua New Guinea	**71.98**
112	Bonaire, Sint Eustatius and Saba	**71.93**
113	Netherlands	**71.93**
114	Mauritius	**71.8**
115	South Africa	**71.78**
116	Romania	**71.77**
117	Georgia	**71.69**
118	Cameroon	**71.32**
119	Monaco	**71.31**
120	Congo (Brazzaville)	**70.6**
121	Bahrain	**70.54**
122	Turks & Caicos	**70.41**
123	Chad	**70.27**
124	Cape Verde	**70.18**
125	Bangladesh	**70.13**
126	Equatorial Guinea	**70.01**
127	Grenada	**69.84**
128	Tuvalu	**69.46**
129	Tunisia	**69.3**
130	Argentina	**69.2**
131	Timor-Leste	**69.13**
132	Indonesia	**68.49**
133	Aruba	**68.39**
134	Cyprus	**68.39**
135	United Arab Emirates	**68.35**
136	Kiribati	**67.93**
137	Israel	**67.83**
138	Egypt	**67.59**
139	Seychelles	**67.56**

Rank.	Country	Score
140	Kazakhstan	**67.53**
141	Cote D'Ivoire	**67.46**
142	Suriname	**67.39**
143	Costa Rica	**67.12**
144	British Virgin Islands	**67.05**
145	Hong Kong	**66.94**
146	Sierra Leone	**66.85**
147	Peru	**66.75**
148	Angola	**66.74**
149	Samoa	**66.68**
150	St Kitts & Nevis	**66.66**
151	Antigua and Barbuda	**66.57**
152	Sao Tome & Prin.	**66.38**
153	Palau	**66.3**
154	Kyrgyzstan	**66.24**
155	Djibouti	**66.24**
156	Benin	**66.06**
157	India	**65.87**
158	Montenegro	**65.56**
159	Dominican Republic	**65.3**
160	St Vincent & Gren	**65.23**
161	Malaysia	**64.99**
162	Tajikistan	**64.83**
163	Curacao	**64.8**
164	Uzbekistan	**64.8**
165	Algeria	**64.79**
166	Serbia	**64.75**
167	El Salvador	**64.74**
168	Guyana	**64.63**

Rank.	Country	Score
169	Mexico	**64.55**
170	Guatemala	**64.54**
171	Thailand	**64.4**
172	Tanzania	**64.19**
173	Eritrea	**64.19**
174	Honduras	**64.15**
175	Moldova	**64.09**
176	St Lucia	**63.99**
177	Belize	**63.89**
178	Comoros	**63.77**
179	Malta	**63.73**
180	Belarus	**63.5**
181	Colombia	**63.31**
182	Ghana	**63.29**
183	Vietnam	**63.26**
184	Armenia	**63.04**
185	Burkina Faso	**62.8**
186	Ecuador	**62.74**
187	Mozambique	**62.6**
188	Turkmenistan	**62.49**
189	Paraguay	**62.25**
190	Kosovo	**62.07**
191	Kenya	**61.83**
192	Nigeria	**61.73**
193	Azerbaijan	**61.63**
194	Guinea	**61.62**
195	Bosnia-Herzegovina	**60.81**
196	Bahamas	**60.43**
197	Dominica	**60.19**

Rank.	Country	Score
198	Bolivia	**59.83**
199	Uganda	**59.41**
200	China	**59.25**
201	Lao People's Democratic Republic	**58.94**
202	Vanuatu	**58.85**
203	Trinidad & Tobago	**58.17**
204	Ukraine	**57.19**
205	Central African Rep	**56.57**
206	Liberia	**56.34**
207	Brazil	**56.3**
208	Russian Federation	**56.2**
209	Gaza Strip	**55.54**
210	West Bank (Palestinian Territory, O	**55.54**
211	Sudan	**55.43**
212	Jordan	**55.37**
213	Cayman Islands	**55.23**
214	Congo, the Democratic Republic	**54.81**
215	Burundi	**54.64**
216	Cuba	**54.28**
217	St Maarten	**53.86**
218	Albania	**53.61**
219	Cambodia	**53.39**
220	Senegal	**52.06**
221	Morocco	**50.31**
222	Western Sahara	**50.31**
223	Barbados	**50.14**
224	Jamaica	**49.64**
225	Guinea Bissau	**47.99**
226	Lebanon	**46.08**

Rank.	Country	Score
227	Philippines	46
228	Venezuela	45.76
229	Mali	45.05
230	Pakistan	44.84
231	Libya	44.62
232	Zimbabwe	44.16
233	Panama	43.84
234	Iraq	43.71
235	Turkey	40.98
236	Somalia	38
237	Nicaragua	37.65
238	Myanmar	36.3
239	South Sudan	36.18
240	Syria	34.89
241	Haiti	33.24
242	Yemen	32.89
243	Afghanistan	32.1
244	North Korea	20.93
245	Iran, Islamic Republic of	17.83

26 Appendix: Sample Location Geographic Risk Analysis Chart (Locations Within Canada)

Location	Location Type (Office or Agent)	% of Total Annual Transaction Volume	% of All STRs Filed in the past year	% of Unusual Transactions escalated to the Compliance Officer in the last year	% of All LCTRS Filed in the last year	% of All Customers and Business Relationships Dealing with the Location	% of All High-risk Customers and Business Relationships	Distance from a Border Crossing in KM	The area is known to have an elevated crime rate	Known Issues with Staff and/or Controls	Other Relevant Risk Factors	Assessed Location Risk (High, Medium, Low)

27 Appendix: Sample High-risk Location Special Controls

Location	Compliance Officer Notes & Rationale	Special Measures Applicable