



# Trackon Canada Private Ltd

## Money Laundering & Terrorist Financing Risk Assessment

**Version Number:** 1.0

**Last Updated:** July 2022

**Next Update:** January 2023

**Approved By:** Jaspreet Singh, Compliance Officer

**Senior Officer Approval for Program:** Jaspreet Singh, Director



## Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>1 Risk Assessment.....</b>	<b>5</b>
<b>2 Money Laundering Risk.....</b>	<b>5</b>
<b>3 Terrorist Financing Risk .....</b>	<b>5</b>
<b>4 What's Risky? .....</b>	<b>5</b>
<b>5 How Do We Assess Risk? .....</b>	<b>6</b>
<b>6 Executive Summary.....</b>	<b>7</b>
6.1 Our Business .....	7
6.2 Our Risk: Business Based Risk Assessment Summary.....	7
<b>7 Our Products, Services &amp; Delivery Channels.....</b>	<b>8</b>
7.1 Products & Services.....	9
7.1.1 Remittance .....	9
7.1.2 Foreign Exchange .....	9
7.2 Payment Methods.....	10
7.2.1 Debit Card.....	10
7.2.2 Electronic Funds Transfers (EFTs) Including Email Money Transfers.....	10
7.3 Delivery Channels .....	11
7.3.1 Non-Face-to-Face Transactions.....	11
<b>8 Geography.....</b>	<b>11</b>
8.1 Destination & Origin of Funds .....	13
8.1.1 Canada.....	13
8.1.2 India .....	14
8.2 Locations Within Canada, Including Our Locations & Customer Locations .	14
<b>9 Customers &amp; Business Relationships.....</b>	<b>15</b>
9.1 Customers That Do Not Form Business Relationships.....	15
9.2 Customers That Form Business Relationships .....	16
9.3 High Risk Customers & Business Relationships.....	16
9.4 Prohibited Customers & Business Relationships .....	17
<b>10 New Developments &amp; Technologies .....</b>	<b>17</b>
<b>11 Other Factors.....</b>	<b>17</b>
11.1 Relevant Operational Processes .....	18
11.2 Employees.....	18
11.3 Financial Services Suppliers (including Correspondent Banks).....	18
11.4 Non-Financial Suppliers.....	18
<b>12 Controls .....</b>	<b>19</b>



<b>13</b>	<b>Products, Services &amp; Delivery Channels Controls .....</b>	<b>19</b>
13.1	Products, Services & Delivery Channel Controls – General.....	19
13.2	Products & Services Controls – General .....	19
13.2.1	Remittance Controls .....	20
13.2.2	Foreign Exchange Controls .....	21
13.3	Payment Methods Controls - General.....	21
13.3.1	Debit Controls.....	21
13.3.2	Electronic Funds Transfer Controls .....	21
13.4	Delivery Channels Controls – General .....	21
13.4.1	Non-Face-to-Face Controls.....	22
<b>14</b>	<b>Geography Controls - General .....</b>	<b>22</b>
14.1	Destination & Origin of Funds Controls .....	22
14.1.1	Canada Controls.....	23
14.1.2	India Controls .....	23
14.2	Locations Within Canada, Including Our Locations & Customer Locations Controls .....	23
<b>15</b>	<b>Customers &amp; Business Relationships Controls.....</b>	<b>23</b>
15.1	Customers That Do Not Form Business Relationships Controls .....	24
15.2	Customers That Form Business Relationships Controls .....	24
15.3	High Risk Customer & Business Relationship Controls.....	24
15.4	Prohibited Customer & Business Relationship Controls .....	25
<b>16</b>	<b>New Developments &amp; Technologies Controls .....</b>	<b>25</b>
<b>17</b>	<b>Other Factor Controls .....</b>	<b>25</b>
17.1	Relevant Operational Process Controls .....	25
17.2	Employee Controls .....	25
17.3	Financial Services Supplier (including Correspondent Banks) Controls.....	26
17.4	Non-Financial Supplier Controls.....	26
<b>18</b>	<b>Customer Based Risk Assessment: Customer &amp; Business Relationship Risk Ranking .....</b>	<b>27</b>
18.1	Business Relationships .....	27
18.2	Customers & Business Relationships That Are Not High Risk .....	27
18.3	High Risk Customers & Business Relationships.....	28
18.4	Prohibited Customers & Business Relationships .....	29
<b>19</b>	<b>Transaction Monitoring &amp; Enhanced Transaction Monitoring .....</b>	<b>29</b>
<b>20</b>	<b>Enhanced Due Diligence .....</b>	<b>30</b>
<b>21</b>	<b>Updates to Customer Information &amp; Identification .....</b>	<b>30</b>
<b>22</b>	<b>Appendix: Compliance Officer References.....</b>	<b>32</b>
22.1	Financial Action Task Force (FATF) .....	32
22.2	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) .....	32
22.3	Know Your Country .....	32
22.4	Office of the Superintendent of Financial Institutions (OSFI) .....	32



<b>23 Appendix: Sample High Risk Customer &amp; Business Relationship Monitoring &amp; Due Diligence Log.....</b>	<b>33</b>
<b>24 Appendix: Country Risk Rating Methodology .....</b>	<b>34</b>
<b>25 Appendix: Country Risk Table.....</b>	<b>35</b>
<b>26 Appendix: Sample Location Geographic Risk Analysis Chart (Locations Within Canada).....</b>	<b>42</b>
<b>27 Appendix: Sample High Risk Location Special Controls.....</b>	<b>43</b>
<b>28 Appendix: Sample High Risk Customer &amp; Business Relationship Risk Factors .....</b>	<b>44</b>



## **Risk Assessment**

Trackon<sup>1</sup> is committed to preventing, detecting, and deterring money laundering and terrorist financing and has a zero-tolerance policy regarding such activities. This document forms part of our anti-money laundering (AML), counter terrorist financing (CTF) program, in conjunction with our training program, policy and procedural documentation.

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.

### **1 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.

### **2 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.

### **3 What's Risky?**

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

---

<sup>1</sup> Throughout our compliance documentation, "we," "our," and "Trackon" are used to refer to Trackon Canada Private Ltd.



- 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.<sup>2</sup> 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.

## 4 How Do We Assess Risk?

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.

We assess the risk in each of these categories as “high risk” and “not high risk.” A score for the entire business is obtained by taking the average risk rating across each of the five categories. To do this, we assign a numeric score to each:

- High = 1
- Not High = 0

We will consider the risk that money laundering or terrorist financing could occur both before our controls have been applied and after our controls have been applied. While high risk before controls have been applied is acceptable (the risk that would exist if there were no controls put in place by Trackon), it is expected that our controls will reduce the risk “after controls” to Not High levels in all

---

<sup>2</sup> Traditional concepts of placement, layering and integration remain critical to identification of money laundering.



categories. Where the risk after controls have been applied is still High, the Compliance Officer will revise the controls.

## **5 Executive Summary**

### **5.1 Our Business**

Trackon is an MSB under Canadian legislation. Trackon's business consists of remittance services between Canadian customers and beneficiaries in India via their website or mobile application. Trackon's customers generally are local residents with the need to send money to their family and friends. The vast majority of customers are expected to be repeat customers.

Remittances transactions are the core of Trackon's business but each transaction has an element of foreign exchange.

Transactions payments may be facilitated in a variety of methods, including:

- Electronic funds transfer (including wires),
- Email money transfers, and
- Debit card.

All funds are received in CAD and paid out in INR. Funds are sent directly to the beneficiary's bank account and local pick up via our trusted payout partners.

Trackon is owned by Jaspreet Singh, who is also the Compliance Officer and has held the position since October 2020. There is one full-time employee focused on Canadian operations.

Trackon does not carry out any business in the province of Quebec nor does Trackon use agents.

### **5.2 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 (1).

Our controls effectively mitigate the risks to our business; the risk that remains once our controls have been applied (our residual risk) is Not High (0).



Category	Before Controls (Inherent) Risk (High/Not High)	Rating (1/0)	After Controls (Residual) Risk (High/Not High)	Rating (1/0)
<b>Products, Services &amp; Delivery Channels</b>	High	1	Not High	0
<b>Geography</b>	High	1	Not High	0
<b>Customers &amp; Business Relationships</b>	High	1	Not High	0
<b>New Developments &amp; Technologies</b>	High	1	Not High	0
<b>Other Factors</b>	High	1	Not High	0
<b>Total</b>	High	1	Not High	0

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.

## 6 Our Products, Services & Delivery Channels<sup>3</sup>

In this section, we consider 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.

The average money laundering and terrorist financing risk related to our products, services and delivery channels, before controls are applied, is High (1).

---

<sup>3</sup> 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 Trackon has applied any controls.





## **6.1 Products & Services**

### **6.1.1 Remittance**

Remittance refers to the transfer of currency between parties or accounts in the jurisdictions in which Trackon operates. Trackon only conducts outgoing remittance transactions (from Canada to India).

Without consideration for specific controls, remittance transactions carry significant money laundering and terrorist financing risks as value can be transferred across jurisdictions (making the transactions more difficult to trace), frequently and in any amount. FINTRAC's guidance indicates that both remittance transactions, and the entities that conduct such transactions, should be considered inherently high risk for money laundering and terrorist financing.

In most jurisdictions, specific regulation applies to remittance transactions, including thresholds at which customers must be identified, and regulatory reporting. This type of regulation is intended to limit the ability of any individual or organization to complete anonymous remittance transactions where there is significant value and/or velocity.

Nonetheless, it is possible to achieve some degree of anonymity by using third parties or corporate structures designed to obfuscate an organization's ownership or control structure. In addition, international remittance transactions may also include a foreign exchange component, further rendering traceability difficult (as the values would need to be matched across multiple currencies).

100% of our customers conduct remittance transactions. The average value of remittance transactions is estimated to be between CAD 20 – 8,000.

The risk of money laundering or terrorist financing through remittance transactions, before controls are applied, is High (1).

### **6.1.2 Foreign Exchange**

Foreign exchange involves the trading of currencies. Like legitimate businesses, criminal networks function internationally and require the exchange of currency in order to conduct business. Foreign exchange transactions may also be conducted for the purpose of obfuscating the source of funds, by creating a complex string of transactions that are difficult to trace. Generally, foreign exchange transactions are conducted through financial networks that include banks, credit unions and MSBs, which are all regulated entities in Canada.

Trackon does not offer standalone foreign exchange services but it is expected that most remittance transactions will contain an element of foreign exchange. The average value of a foreign exchange transaction is expected to be the same as a remittance transaction.



The risk of money laundering or terrorist financing through foreign exchange, before controls are applied, is High (1).

## **6.2 Payment Methods**

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

- Debit; and
- Electronic Funds Transfers (EFTs), including wires and email money transfers.

Additional payment methods may be added over time. They will be added to this risk assessment before they are implemented. An assessment of the risk related to each method of payment that we accept appears below.

Based on the average risk of all payment methods that we accept, the risk of money laundering or terrorist financing, before controls are applied, is High (1).

### **6.2.1 Debit Card**

Acquiring a debit card requires interacting with and being identified by a financial institution. Debit card transactions require a personal identification number to confirm the transaction. Online debit card transactions require specific information, such as the cardholder's address and a card number, and may also require a separate password to authorize the transaction. Debit card transactions are tracked and monitored by financial institutions. Debit cards cannot be easily anonymously transferred between individuals.

However, a debit card may be used by an individual who is aware of the personal identification number (PIN) and/or other specific information, whether or not that individual owns the card.

It is estimated that roughly 50% of our business is conducted by Debit cards with the average transaction value being between CAD 20 – 8,000.

The risk of money laundering and terrorist financing related to debit card payments, before controls are applied, is Not High (0).

### **6.2.2 Electronic Funds Transfers (EFTs) Including Email Money Transfers**

Sending funds via electronic funds transfer (EFT), including email transfers and wires, generally requires an accountholder relationship with a financial institution. In establishing an account, the customer is identified, and all transactions are tracked and monitored. Although these transactions cannot be completed anonymously, funds transfers, in particular international funds transfers, can be used to move funds from person to person or country to country relatively quickly.

It is estimated that roughly 50% of our business is conducted by EFT with the average transactions value being between CAD 20 – 8,000.



The risk of money laundering and terrorist financing related to electronic funds transfers, including email money transfers and EFTs, before controls are applied, is High (1).

### **6.3 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 customers via:

- Word of mouth (from existing customers);
- Radio advertisement;
- Web advertisement and website; and
- Social media.

Currently, we only serve our customers non-face-to-face via our website, email or phone.

Taken together, the risk of money laundering or terrorist financing via our delivery channels, before controls are applied, is High (1).

#### **6.3.1 Non-Face-to-Face Transactions**

Trackon customers are able to conduct transactions online via our website and mobile app. Since we do not meet with customers face-to-face, there is less opportunity to understand our customers and their transactions. Therefore, staff is trained to spot anomalies and indicators of potentially suspicious transactions.

100% of our transactions are conducted non-face-to-face. The average transaction value is estimated to be between CAD 20 – 8,000.

The risk of money laundering or terrorist financing related to non-face-to-face transactions, before controls are applied, is High (1).

## **7 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)<sup>4</sup> and materials published by

---

<sup>4</sup> <http://www.fatf-gafi.org/>



KnowYourCountry.com<sup>5</sup> that describe money laundering and terrorist financing risk related to particular countries.

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

Not High	High
$\geq 50$	$< 50$

The FATF's publications include a list of high risk and non-cooperative countries (countries that have not developed AML and CTF regimes or that have not made sufficient progress in developing AML and CTF regimes)<sup>6</sup>.

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.

Additional High Risk countries include:

- Albania;
- Bahamas;
- Barbados;
- Botswana;
- Cambodia;
- Ghana;
- Jamaica;
- Mauritius;
- Myanmar;
- Nicaragua;
- Pakistan;
- Panama;
- Syria;
- Uganda;
- Yemen; and
- Zimbabwe.

---

<sup>5</sup> A full description of the Know Your Country methodology is included in an appendix to this document.

<sup>6</sup> <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/>



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 supplies from high risk jurisdictions.

Where our customer or supplier is located in high risk jurisdictions, we consider the situation to be higher risk and ensure that appropriate controls are applied.

The risk of money laundering or terrorist financing related to Trackon's geography, before controls are applied, is Not High (0).

### **7.1 Destination & Origin of Funds**

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

- Canada (Not High Risk); and
- India (Not High Risk).

The Know Your Country 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 Trackon's transactions.

The risk of money laundering or terrorist financing related to Trackon's destination and origin of funds locations, before controls are applied, is Not High (0).

#### **7.1.1 Canada**

Our customers are located in Canada, which according to [knowyourcountry.com](https://www.knowyourcountry.com) is rated 75.22/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 78th of the 129 countries included)<sup>7</sup>.

Additionally, when compared to other countries within the Americas (North, Central and South America), Canada is considered to have the lowest crime index (ranked 25th of the 26 countries included)<sup>8</sup>.

---

<sup>7</sup> [https://www.numbeo.com/crime/rankings\\_by\\_country.jsp](https://www.numbeo.com/crime/rankings_by_country.jsp)



All (100%) of Trackon's transactions involve Canada.

The money laundering and terrorist financing risk related to Canada, before controls are applied, is Not High (0).

### **7.1.2 India**

The majority of our customers' beneficiaries are located in India, which according to knowyourcountry.com is rated 66.02/Not High.

India'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. "The last Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards in India was undertaken by the Financial Action Task Force (FATF) in 2010. According to that Evaluation, India was deemed Compliant for 4 and Largely Compliant for 25 of the FATF 40 + 9 Recommendations. It was Partially Compliant or Non-Compliant for 5 out of the 6 Core Recommendations<sup>9</sup>."

All (100%) of Trackon's transactions involve India.

The money laundering and terrorist financing risk related to India, before controls are applied, is Not High (0).

## **7.2 Locations Within Canada, Including Our Locations & Customer Locations**

Trackon's head office is in Mississauga Canada. The current location is not known to be a high crime area<sup>10</sup>.

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,
- % 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,

---

<sup>8</sup>[https://www.numbeo.com/crime/rankings\\_by\\_country.jsp?title=2020&region=01](https://www.numbeo.com/crime/rankings_by_country.jsp?title=2020&region=01)

<sup>9</sup> <https://www.knowyourcountry.com/india1111>

<sup>10</sup> <https://www.numbeo.com/crime/in/Toronto>



- 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 or Not High 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, Not High)
4440 5 street NW Edmonton AB T6T0Z9	Head Office	100%	100%	100%	100%	Within 150 kms	No	No	Major urban centre, close to an international airport.	Not High

The risk of money laundering and terrorist financing related to Trackon's location, before controls are applied, is Not High (0).

## 8 Customers & Business Relationships

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

- Customers That Do Not Form Business Relationships;
- Customers That Form Business Relationships;
- High Risk Customers & Business Relationships; and
- Prohibited Customers & Business Relationships.

The risk of money laundering and terrorist financing related to our customers and business relationships, before controls are applied, is High (1).

### 8.1 Customers That Do Not Form Business Relationships

Customers that do not form business relationships refers to customers that have not conducted two or more transactions that require identification within the past five



years, or a business with which we do not have an ongoing service agreement. These customers are considered to be “Not High” risk.

While most customers are repeat customers, the majority of our customers do not meet the threshold for the formation of business relationships given transaction amounts.

These customers provide complete KYC information, are verified and/or identified as required, and have not recently requested or completed transactions that we have reasonable grounds to believe are related to money laundering or terrorist financing.

While many of our customers are repeat customers, we expect the majority to not meet the threshold of a business relationship based on transactions amounts completed.

The money laundering or terrorist financing risk related to our customers that do not form business relationships, before controls are applied, is Not High (0).

## **8.2 Customers That Form Business Relationships**

Customers that form business relationships refers to customers who conduct two or more transactions which require identification, within a five year span or any customer who is an entity that we have an ongoing service agreement with. As it pertains to our business, it can be any combination of:

- Any customer with whom we have an ongoing service agreement with;
- Remittance transactions with a value of CAD 1,000 or more; and/or
- Transactions resulting in an STR or ASTR reported to FINTRAC.

While many of our customers are repeat customers, we expect a very small percent to meet the threshold of a business relationship based on transactions amounts completed.

The money laundering or terrorist financing risk related to our customers that form business relationships, before controls are applied, is Not High (0).

## **8.3 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. This includes instances where we have filed a Suspicious Transaction Report (STR) or an Attempted Suspicious Transaction Report (ASTR) with FINTRAC.

A very small portion of our customers (less than five percent) 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 (1).

#### **8.4 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:

- Shell banks;
- Shell companies and/or companies that do not appear to serve any legitimate economic purpose;
- 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 Trackon 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 (1).

### **9 New Developments & Technologies**

As an existing business moving into Canada, the launch of the Canadian business and all related technologies and compliance related recordkeeping systems have been tested, vetted and are currently in operation. However, the obligations in Canada are different. As such, there is a higher risk of failures and/or outages until such systems are proven to be operating effectively.

The money laundering and terrorist financing risk related to new developments and technologies, before controls are applied, is High (1).

### **10 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.



The average money laundering and terrorist financing risk related to our other factors, before controls are applied, is High (1).

### **10.1 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 (1).

### **10.2 Employees**

Employees for the purpose of this risk assessment include full and part time staff, as well as contract and seasonal 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.

Trackon currently have 1 full-time employee. New hires are expected as we grow.

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

### **10.3 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.

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 (1).

### **10.4 Non-Financial Suppliers**

Our suppliers of non-financial services include IT service providers, consultants, and accountants. 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 Not High (0).

## **11 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 Trackon's business as a whole. Specific regional processes are described in the Compliance Procedures for each region in which we operate.

## **12 Products, Services & Delivery Channels Controls**

### **12.1 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.
- 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 Not High (0).

### **12.2 Products & Services Controls – General**

- Trackon 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<sup>11</sup>.
- Transaction limits apply to each transaction.
- 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 probing questions.
- 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.

The residual risk (after controls have been applied) is Not High (0).

#### **12.2.1 Remittance Controls**

- Complete sender and beneficiary information is recorded for all transactions.
- We do not conduct transactions that involve countries listed as non-cooperative by the FATF and/or countries deemed to be of "extreme" risk.
- Transactions involving countries deemed too high risk are rejected automatically by our IT system.
- Transactions involving countries deemed to be of high risk are flagged for manual review and may be rejected (based on the results of manual review).
- The Compliance Officer maintains an up to date knowledge of the money laundering and terrorist financing risks for the jurisdictions which Trackon does business with, and will apply specific controls to mitigate potential issues where risks are elevated.
- All customers and beneficiaries are list screened.
- All transactions that require a customer to be identified are approved by hour Compliance Officer.

The residual risk (after controls have been applied) is Not High (0).

---

<sup>11</sup> In some cases, Trackon, based on Trackon's risk tolerance, establishes thresholds. In other instances, thresholds are based on jurisdictional transaction limits established by local governments or banking service providers.



### **12.2.2 Foreign Exchange Controls**

- Foreign exchange transactions are performed only as a function of remittance transactions; no standalone/over the counter foreign exchange transactions are conducted. All controls applicable to remittance transactions are applicable to foreign exchange transactions.

The residual risk (after controls have been applied) is Not High (0).

### **12.3 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 Not High (0).

#### **12.3.1 Debit Controls**

- Card payments are accepted only from the individual that owns the card.
- All debit card transactions require a form of authentication (such as chip and PIN) to complete.
- Where card authentication fails, the transaction cannot be completed.
- If there is doubt about the card's ownership, identification documents may be requested.

The residual risk (after controls have been applied) is Not High (0).

#### **12.3.2 Electronic Funds Transfer Controls**

- The origin of EFTs is verified, where possible, and if the payment appears to have originated from someone other than our customer, the Compliance Officer is notified and additional questions are asked.

The residual risk (after controls have been applied) is Not High (0).

### **12.4 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 Not High (0).



#### **12.4.1 Non-Face-to-Face Controls**

- Records of all customer transactions are maintained, including the customer's KYC information.
- The identification on file must be up to date for transactions.
- All transactions that we process are entered into our recordkeeping system.
- We do not conduct off the record transactions under any circumstances.
- All of our staff are trained to recognize transactions that may be related to money laundering and/or terrorist financing and to report these to the Compliance Officer as soon as possible.

The residual risk (after controls have been applied) is Not High (0).

### **13 Geography Controls - General**

- Trackon 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 Not High (0).

#### **13.1 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 Trackon'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 Not High (0).



### **13.1.1 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.

The residual risk (after controls have been applied) is Not High (0).

### **13.1.2 India Controls**

- All payouts take place via direct deposit to a bank account.

The residual risk (after controls have been applied) is Not High (0).

## **13.2 Locations Within Canada, Including Our Locations & Customer 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.
- Trackon does not operate locations in jurisdictions that have been deemed to be non-cooperative by the FATF.
- 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 Not High (0).

## **14 Customers & Business Relationships Controls**

- All customers and business relationships are required to provide know your customer (KYC) information and identification.
- 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 Not High (0).

#### **14.1 Customers That Do Not Form Business Relationships Controls**

- Customers that cannot be identified are blocked from completing any qualifying transactions.
- Customers are identified (where possible) when there is any suspicion of money laundering or terrorist financing (regardless of the transaction amount or whether the transaction is actually completed).
- Identification information and other client records are maintained for at least five (5) years.
- If there is any doubt about the identification documents or other documents that a client provides, additional documents will be requested.
- All customers and beneficiaries are screened against publicly available sanctions lists.

The residual risk (after controls have been applied) is Not High (0).

#### **14.2 Customers That Form Business Relationships Controls**

- All measures that are applied to customers that do not form business relationships are applied.
- The intended nature and purpose of the business relationship is recorded and used by the Compliance Officer in order to conduct transaction monitoring.

The residual risk (after controls have been applied) is Not High (0).

#### **14.3 High Risk Customer & Business Relationship Controls**

- All measures that are applied to customers that do not form business relationships, and customers that form 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 Not High (0).

#### **14.4 Prohibited Customer & Business Relationship Controls**

- All potential customers are screened against terrorist watch lists, 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.

The residual risk (after controls have been applied) is Not High (0).

### **15 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.
- All new systems are thoroughly tested before implementation.
- A risk assessment is performed and documented prior to any new procedures or operations are implemented.

The residual risk (after controls have been applied) is Not High (0).

### **16 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.
- Trackon has in place a security policy.

The residual risk (after controls have been applied) is Not High (0).

#### **16.1 Relevant Operational Process Controls**

- Trackon'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.
- Trackon'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 Not High (0).

#### **16.2 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.
- The applicant must be recommended to us by an individual that is trustworthy and known to us.
- The applicant is interviewed by the manager/President.
- The applicant's contact information and personnel information are obtained.

The residual risk (after controls have been applied) is Not High (0).

### **16.3 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 Not High (0).

### **16.4 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 Not High (0).



## **17 Customer Based Risk Assessment: Customer & Business Relationship Risk Ranking**

We divide our customers and business relationships into High and Not High risk buckets based on their activities.

High risk customers are maintained within our IT system and changes over time based on the customer's characteristics, beneficiary countries, and transaction activity.

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.

### **17.1 Business Relationships**

We have a business relationship with any customer that has completed two or more transactions that require the customer to be identified.

In these cases, we must collect and record information about the "nature and purpose" of that business relationship. As of June 1, 2021 we will also have to conduct a Politically Exposed Person (PEP) or Head of an International Organization (HIO) determination when we enter into a business relationship with a customer.

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.

### **17.2 Customers & Business Relationships That Are Not High Risk**

Most of our customers and 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 "Not High."

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 Trackon).



In rare instances, a customer or business relationship may be moved out of the high or prohibited risk categories. 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 Trackon. In such cases, a detailed rationale must be documented.

### **17.3 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. These include customers for whom:

- The client frequently uses wire transfers for no apparent reason;
- The client appears outside of our normal customer base;
- Trackon is aware that the customer is under investigation by a regulator;
- A positive match has been indicated for the customer under the listing screening procedures;
- Trackon is aware that an individual customer is a Politically Exposed Foreign Person (PEFP);
- 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;
- 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 Business, 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.

The Compliance Officer maintains knowledge of high risk customers. A sample high risk customer log can be found in an appendix to this document.

#### **17.4 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:

- Shell banks;
- Shell companies and/or companies that do not appear to serve any legitimate economic purpose;
- 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 Trackon 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.

### **18 Transaction Monitoring & Enhanced Transaction Monitoring**

The Compliance Officer or a designate, monitors transactions for potentially suspicious transactions using ComplyAdvantage<sup>12</sup>. 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 annually, and more frequently where triggered by customer activity (for example, where there is an internal report submitted to the Compliance Officer).

---

<sup>12</sup> <https://complyadvantage.com/aml-transaction-monitoring/>



The Compliance Officer will maintain complete records of the reviews and maintain these records for at least five years.

A sample High Risk Customer & Business Relationship monitoring log can be found in an appendix to this document. All monitoring activities are captured on this log until our IT system functionally is built where at that time, notes about compliance monitoring activities for customers will be housed in our IT systems.

## **19 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 will 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)<sup>13</sup> and the Royal Canadian Mounted Police (RCMP)<sup>14</sup>).

Additional enhanced due diligence activities may apply according to the customer's risk characteristics (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.

## **20 Updates to Customer Information & Identification**

All active customers<sup>15</sup> 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:

---

<sup>13</sup> <https://www.canada.ca/en/security-intelligence-service.html>

<sup>14</sup> <http://www.rcmp-grc.gc.ca/en/home>

<sup>15</sup> Active customer means any customer that has conducted a transaction within the past year.



- High Risk – at least every two years;
- Not High Risk – at least every five years.

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.



## **21 Appendix: Compliance Officer References**

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

### **21.1 Financial Action Task Force (FATF)**

[www.fatf-gafi.org/](http://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).

### **21.2 Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**

[www.fintrac-canafe.gc.ca](http://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.

### **21.3 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.

### **21.4 Office of the Superintendent of Financial Institutions (OSFI)**

[www.osfi-bsif.gc.ca](http://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.

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



## 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<sup>16</sup>

Last updated November 4, 2020

Not High		High	
≥50		<50	

	Country	Score
1	Norway	87.49
2	Svalbard and Mayen	87.49
3	Sweden	87.49
4	Åland Islands	86.75
5	Finland	86.75
6	New Zealand	85.81
7	Tokelau	85.81
8	Denmark	85.61
9	Faroe islands	85.61
10	Greenland	85.61
11	Estonia	84.48
12	Iceland	84.15
13	Slovenia	83.81
14	Bermuda	83.34
15	Lithuania	83.22
16	Andorra	82.26
17	Malta	82.14
18	San Marino	81.89
19	Oman	80.06
20	Austria	80.03
21	Croatia	79.92
22	Namibia	78.38

<sup>16</sup> <https://www.knowyourcountry.com/country-ratings-table>



23	Vatican City State (Holy See)	77.99
24	Burkina Faso	77.83
25	Germany	77.8
26	South Korea	77.6
27	France	77.57
28	French Guiana	77.57
29	French Polynesia	77.57
30	Guadeloupe	77.57
31	Martinique	77.57
32	Mayotte	77.57
33	New Caledonia	77.57
34	Réunion	77.57
35	Saint Berthélemy	77.57
36	Saint Martin (French part)	77.57
37	Saint Pierre and Miquelon	77.57
38	Wallis and Futuna	77.57
39	Montserrat	77.55
40	Bhutan	77.41
41	Macedonia	77.24
42	Rwanda	77.09
43	Malawi	76.94
44	Brunei Darussalam	76.91
45	Singapore	76.83
46	Tonga	76.82
47	Australia	76.78
48	Christmas Island	76.78
49	Cocos (Keeling) Islands	76.78
50	Norfolk Island	76.78
51	Solomon Islands	76.73
52	Switzerland	76.68
53	Zambia	76.67
54	Czech Republic	76.49
55	Guernsey	76.44
56	Chile	76.1
57	Fiji	76.08
58	Anguilla	76
59	Belgium	75.9
60	Latvia	75.86
61	Ireland	75.63



62	Niue	75.52
63	Mongolia	75.43
64	Liechtenstein	75.43
65	Greece	75.38
66	Jersey	75.38
67	Spain	75.24
68	Canada	75.22
69	Qatar	75.19
70	North Mariana Islands	75
71	United States	75
72	Luxembourg	74.78
73	Poland	74.74
74	Taiwan	74.69
75	Isle Of Man	74.65
76	Portugal	74.38
77	Slovakia	74.29
78	British Indian Ocean Territory	74.29
79	Falkland Islands (Malvinas)	74.29
80	Pitcairn	74.29
81	Saint Helena, Ascension and Trista	74.29
82	United Kingdom	74.29
83	Hungary	74.24
84	Uruguay	74.1
85	Lesotho	73.92
86	Bulgaria	73.57
87	Marshall Islands	73.24
88	Niger	73.22
89	South Africa	73.17
90	Micronesia	73.14
91	American Samoa	72.95
92	Madagascar	72.91
93	Togo	72.84
94	Nepal	72.69
95	Cook Islands	72.6
96	Gabon	72.48
97	Italy	72.38
98	Mauritania	72.14
99	Kuwait	72.14



<b>100</b>	Gibraltar	72.02
<b>101</b>	Bonaire, Sint Eustatius and Saba	71.92
<b>102</b>	Netherlands	71.92
<b>103</b>	Georgia	71.83
<b>104</b>	Romania	71.73
<b>105</b>	Nauru	71.65
<b>106</b>	Papua New Guinea	71.53
<b>107</b>	Sri Lanka	71.4
<b>108</b>	Ethiopia	71.36
<b>109</b>	Cameroon	71.35
<b>110</b>	Monaco	71.33
<b>111</b>	United States Virgin Islands	70.97
<b>112</b>	Swaziland (Eswatini)	70.52
<b>113</b>	Turks & Caicos	70.41
<b>114</b>	Congo (Brazzaville)	70.3
<b>115</b>	Chad	70.26
<b>116</b>	Bahrain	70.21
<b>117</b>	Equatorial Guinea	70.13
<b>118</b>	Gambia	70.12
<b>119</b>	Hong Kong	70.04
<b>120</b>	Bangladesh	69.97
<b>121</b>	Grenada	69.92
<b>122</b>	Macau	69.74
<b>123</b>	Costa Rica	69.64
<b>124</b>	Argentina	69.56
<b>125</b>	Cyprus	69.45
<b>126</b>	Puerto Rico	69.12
<b>127</b>	Indonesia	69.04
<b>128</b>	Jordan	68.9
<b>129</b>	Timor-Leste	68.88
<b>130</b>	Saudi Arabia	68.85
<b>131</b>	Israel	68.71
<b>132</b>	Tuvalu	68.67
<b>133</b>	Guyana	68.66
<b>134</b>	Aruba	68.6
<b>135</b>	United Arab Emirates	68.38
<b>136</b>	Maldives	68.34
<b>137</b>	Cayman Islands	68.08



<b>138</b>	Suriname	68.03
<b>139</b>	Kiribati	67.79
<b>140</b>	Guam	67.77
<b>141</b>	Cote D'Ivoire	67.57
<b>142</b>	Djibouti	67.29
<b>143</b>	Malaysia	67.23
<b>144</b>	British Virgin Islands	67.05
<b>145</b>	St Kitts & Nevis	66.85
<b>146</b>	Sierra Leone	66.75
<b>147</b>	Palau	66.69
<b>148</b>	Japan	66.68
<b>149</b>	Angola	66.54
<b>150</b>	Antigua and Barbuda	66.48
<b>151</b>	Peru	66.47
<b>152</b>	Kazakhstan	66.32
<b>153</b>	Sao Tome & Prin.	66.31
<b>154</b>	Senegal	66.02
<b>155</b>	India	66.02
<b>156</b>	Cape Verde	65.8
<b>157</b>	Kyrgyzstan	65.53
<b>158</b>	St Vincent & Gren	65.25
<b>159</b>	Serbia	65.06
<b>160</b>	Seychelles	64.99
<b>161</b>	Vanuatu	64.87
<b>162</b>	Curacao	64.8
<b>163</b>	Algeria	64.76
<b>164</b>	Thailand	64.65
<b>165</b>	Dominican Republic	64.63
<b>166</b>	Montenegro	64.62
<b>167</b>	Honduras	64.56
<b>168</b>	Tajikistan	64.46
<b>169</b>	Eritrea	64.42
<b>170</b>	El Salvador	64.39
<b>171</b>	Trinidad & Tobago	64.37
<b>172</b>	Belize	64.17
<b>173</b>	Benin	64.1
<b>174</b>	Uzbekistan	64.03
<b>175</b>	Moldova	63.73
<b>176</b>	Mexico	63.72



177	Vietnam	63.46
178	St Lucia	63.44
179	Mauritius - on FATF AML Def List	63.39
180	Botswana - on FATF AML Def List	63.34
181	Dominica	63.04
182	Colombia	62.99
183	Turkmenistan	62.73
184	Tanzania	62.53
185	Belarus	62.49
186	Kosovo	62.23
187	Paraguay	62.17
188	Armenia	61.5
189	Kenya	61.44
190	Guinea	61.42
191	Mozambique	61.09
192	Samoa	61.05
193	Guatemala	60.5
194	Bolivia	60.17
195	Comoros	60.09
196	Philippines	59.82
197	Tunisia	59.3
198	Morocco	59.3
199	Western Sahara	59.3
200	Cuba	59.27
201	Mali	59.22
202	Lao People's Democratic Republic	59.03
203	Uganda	59.02
204	China	58.83
205	Ecuador	58.35
206	Liberia	56.99
207	Azerbaijan	56.95
208	Egypt	56.75
209	West Bank (Palestinian Territory, O	56.65
210	Ukraine	56.52
211	Central African Rep	56.51
212	Russian Federation	56.01
213	Brazil	56





<b>214</b>	Gaza Strip	55.79
<b>215</b>	Nigeria	55.34
<b>216</b>	Turkey	55.03
<b>217</b>	St Maarten	54.46
<b>218</b>	Burundi	54.05
<b>219</b>	Albania	53.81
<b>220</b>	Sudan	53.2
<b>221</b>	Cambodia	53.05
<b>222</b>	Bahamas	52.17
<b>223</b>	Bosnia-Herzegovina	52.17
<b>224</b>	Jamaica	51.35
<b>225</b>	Ghana	50.65
<b>226</b>	Congo, the Democratic Republic	49.93
<b>227</b>	Guinea Bissau	48.42
<b>228</b>	Haiti	48.09
<b>229</b>	Barbados	47.95
<b>230</b>	Lebanon	46.31
<b>231</b>	Venezuela	45.83
<b>232</b>	Zimbabwe	44.83
<b>233</b>	Libya	44.68
<b>234</b>	South Sudan	44.52
<b>235</b>	Panama	43.96
<b>236</b>	Iraq	43.57
<b>237</b>	Pakistan	42.74
<b>238</b>	Somalia	37.8
<b>239</b>	Nicaragua	36.79
<b>240</b>	Myanmar	36.18
<b>241</b>	Syria	34.85
<b>242</b>	Yemen	32.84
<b>243</b>	Afghanistan	31.83
<b>244</b>	North Korea	20.8
<b>245</b>	Iran, Islamic Republic of	18.01



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

Assessed Location Risk (High, Not High)					
Other Relevant Risk Factors					
Known Issues with Staff and/or Controls					
The area is known to have an elevated crime rate					
Distance from a Border Crossing in KM					
% of All High Risk Customers and Business Relationships					
% of All Customers and Business Relationships Dealing with the Location					
% of All LCTRS Filed in the last year					
% of Unusual Transactions escalated to the Compliance Officer in the last year					
% of All STRs Filed in the past year					
% of Total Annual Transaction Volume					
Location Type (Office or Agent)					
Location					



## 27 Appendix: Sample High Risk Location Special Controls

Location	Compliance Officer Notes & Rationale	Special Measures Applicable



## 28 Appendix: Sample High Risk Customer & Business Relationship Risk Factors

The actual parameters and related ratings will be housed in our IT systems.

Risk Category	Factor	Permanent or Dynamic	Automatic High Risk (HR)	Notes
Customers & Business Relationships	Politically Exposed Foreign Person (outside of Canada)	Permanent	Yes	Senior Officer approval is required within 30 days for any transactions of CAD 100,000 or more.
Customers & Business Relationships	Heads of International Organizations (HIOs)	Permanent	Yes	Senior Officer approval is required within 30 days for any transactions of CAD 100,000 or more.
Customers & Business Relationships	Politically Exposed Person (In Canada) – Federal	Dynamic	Yes	High risk designation lasts for five years from the date that the office was last held.
Customers & Business Relationships	Politically Exposed Person (In Canada) - Provincial or Territorial	Dynamic	No	High risk designation lasts for five years from the date that the office was last held. The PEP may be considered high risk if there are other factors such as large or frequent transactions.
Customers & Business Relationships	Politically Exposed Person (In Canada) – Municipal	Dynamic	No	High risk designation lasts for five years from the date that the office was last held. The PEP may be considered high risk if there are other factors such as large or frequent transactions.
Other	Customer is an employee or	Dynamic	Yes	High risk designation lasts for 1 year following the



<b>Risk Category</b>	<b>Factor</b>	<b>Permanent or Dynamic</b>	<b>Automatic High Risk (HR)</b>	<b>Notes</b>
	contractor with significant system access			termination of employment or contract.
Products, Services & Delivery Channels	Attempted Suspicious or Suspicious Transaction Report (ASTR/STR/VIR)	Dynamic	No	<p>When an ASTR/STR or VIR is filed, the customer is designated as being high risk for two years.</p> <p>The Compliance Officer may lower the risk where there is additional information to support this, however, the rationale for such decisions must be documented in detail.</p> <p>This designation lasts for 1 year from the date that the last STR or ASTR is filed.</p>
Products, Services & Delivery Channels	Cumulative ASTRs/STR/VIRs	Permanent	Yes	<p>If more than 3 ASTRs, STRs or VIRs have been filed, the customer is designated as high risk. The Compliance Officer will consider closing the account.</p> <p>If the account is kept open, the rationale for the decision will be documented and the account will receive a permanent high risk designation.</p>
Products, Services & Delivery Channels	Excessive Cash	Dynamic	No	Where cash is used at different locations, or in amounts that are unusual given the information that is known about the



<b>Risk Category</b>	<b>Factor</b>	<b>Permanent or Dynamic</b>	<b>Automatic High Risk (HR)</b>	<b>Notes</b>
				customer, the customer is considered to be high risk. This designation lasts for 2 years following the last attempt to fund a transaction with cash.
Customers & Business Relationships	High Risk Occupation or Principal Business	Dynamic	Yes	Customer has an occupation or principal business type that is deemed to be high risk.  This designation lasts until the occupation or principal business changes.