Trackon Canada Private Limited

KYC/Customer Due Diligence

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By: Jaspreet Singh, Director

Senior Officer Approval for Program: Jaspreet Singh, Director.

TABLE OF CONTENT

1 Policy Statement

1.1 Our Commitment

Reading this policy and our all-staff procedure is required for all new customers. An attestation confirming that the policy and procedure are read and understood is kept as a KYC record. There are also manual KYC methods for those customers who get rejected by our auto-system of KYC, which includes manual verification of their name, email, contact number, identity card, and their live captured image.

1.2 Purpose

The purpose of the KYC Due diligence Policy is to provide direction to design and implement appropriate controls to meet statutory, legal, regulatory, and contractual requirements within the business functions of the Organization. Additionally, this policy aims to ensure verification & risk controls of all the customers & new customers' information processing systems. By following Security standards it minimizes interference to business operations from the verification process through appropriate planning.

1.3 Scope

The KYC Due Diligence Policy applies to all the customers of Trackon Canada Pvt Ltd.

2 KYC Statement

Trackon Canada Pvt Ltd Canada Pvt Ltd takes effective measures for KYC Due Diligence (know your customer due diligence) to gather information and data in order to verify the identity of customers and make sure that they are not involved with money laundering or another type of financial crime. Trackon Canada Pvt Ltd Canada Pvt Ltd ensures to:

- Establish the identity of the customer.
- Understand the nature of the customer's activities
- Assess money laundering risks associated with that customer to monitor their activity

2.1 KYC Process

The customer is required to complete the KYC process while signing up for our application for the first time. They have to submit their identity proofs by capturing a live picture of a document along with a live selfie for facial recognition. This data is submitted to ONFIDO which in turn verifies the authenticity of the submitted document through their database. The customers then are checked for PEP, Sanctions listings, AML, and CTF. Onfido then automatically either approves the KYC or rejects them and the customer is notified by Onfido directly. Customer verification was completed on all parties seeking to establish an account relationship.

2.2 KYC Records

The evidence of customer verification and KYC is maintained on ONFIDO's dashboard together with our database. The records are retained as per the laws in place for every country.

3 Customers & Business Relationships

Our customers are generally individuals and businesses conducting transactions involving the jurisdictions that we service, who are looking for rates and

settlements 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).

3.1 Customers That Do Not Form Business Relationships

Customers that do not form business relationships refer 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 do not meet the threshold of a business relationship based on transaction 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).

3.2 Customers That Form Business Relationships

Customers that form business relationships refer to customers who conduct two or more transactions that require identification, within five years 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;
- Remittance transactions with a value of CAD 1,000 or more; and
- Transactions resulting in an STR or ASTR are reported to FINTRAC.

While many of our customers are repeat customers, we expect a very small percentage to meet the threshold of a business relationship based on transaction 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).

3.3 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).

3.4 Prohibited Customers & Business Relationships

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

- Shell banks;
- Shell companies and/or companies that do not appear to serve any legitimate economic purpose;
- Any person or entity is known to be involved in money laundering and/or terrorist financing-related activities;
- Any person or entity believed to be attempting to use Trackon Canada Pvt Ltd to conduct or be paid for illegal activities; and
- Any person or entity that has 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).

4 PEP & HIO Checks

As of June 1, 2021, for customers with whom we have entered into a business relationship, or for international EFTs valued at CAD 100,000 or more, we must take reasonable measures to verify whether or not our customer is a politically exposed person (PEP), the head of an international organization (HIO) or the family member or close associate of a domestic PEP (collectively referred to as PEPs for the remainder of this section, unless otherwise specified). Currently, while not required, we conduct such checks at onboarding and periodically throughout the relationship with the customer.

PEPs may be foreign or domestic. The standards that apply will be slightly different, depending on whether the position that the person holds, or has held was within Canada (domestic) or outside of Canada (foreign).

Politically Exposed Foreign Persons (PEFPs), include anyone who holds or has held any of the following offices or positions in or on behalf of a foreign state:

- Head of state or head of government;
- Member of the executive council of government or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counselor of an ambassador;
- Military officer with a rank of general or above;
- President of a state-owned company or a state-owned bank;
- Head of a government agency;
- Judge of a supreme court, constitutional court, or other courts of last resort;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

A person determined to be a foreign PEP is forever a foreign PEP (even after they no longer hold the position).

Domestic Politically Exposed Persons (PEPs) include anyone that holds or has held one of the offices or positions on behalf of the federal government or a provincial government:

- Governor General, lieutenant governor, or head of government;
- Member of the Senate or House of Commons or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counselor of an ambassador;
- Military officer with a rank of general or above;
- President of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- Head of a government agency;
- Judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

It also includes anyone that holds or has held one of the following offices or positions in a municipal government:

- Mayor.

A person ceases to be a domestic PEP 5 years after they have left office.

The head of an international organization is a person who is either:

- The head of an international organization established by the governments of states; or
- The head of an institution established by an international organization.

If the organization was established by means of a formally signed agreement between the governments of more than one country, then the head of that organization is an HIO. The head of an international organization or the head of an institution established by an international organization is the primary person who leads that organization, (i.e. a president or CEO).

In addition to PEFPs, PEPs and HIOs, we consider prescribed family members of such persons that we know are closely associated, for personal or business reasons, with a politically exposed person or HIO as high-risk customers.

Prescribed family members include:

- Mother or father;
- Child;
- Spouse or common-law partner;
- Spouse's or common-law partner's mother or father;
- Brother;
- Sister; and
- Half-brother or half-sister (that is, any other child of the individual's mother or father).

Persons that are closely connected include:

- Business partners with, or who beneficially owns or controls a business with, a PEP or HIO;
- In a romantic relationship with a PEP or HIO, such as a boyfriend, girlfriend, or mistress;
- Involved in financial transactions with a PEP or an HIO;
- A prominent member of the same political party or union as a PEP or HIO;
- Serving as a member of the same board as a PEP or HIO; or
- Closely carrying out charitable works with a PEP or HIO.

When a Trackon Canada Pvt Ltd employee is aware that our customer is a PEFP, PEP, or HIO they will notify the Compliance Officer immediately so that they can perform a risk assessment and adjust the customer's risk ranking accordingly. Foreign PEPs, their family members, and close associates are automatically considered high-risk customers.

When a risk assessment is required for a domestic PEP or HIO, the Compliance Officer will conduct a negative media search to determine if the domestic PEP should be considered low or high risk. Record of the risk assessment should be stored electronically.

If a customer is determined to be a PEP or HIO, the Compliance Officer will ensure that Senior Management is aware of the account and has approved the customer or business relationship within 30 days of the PEP or HIO determination.

The Compliance Officer must keep a record after we have determined that a person is a PEFP, a high-risk HIO, a PEP, a family member, or a close associate of one of these. The record must include:

- The office or position of the PEP or HIO;
- The name of the organization or institution of the PEP or HIO;
- The source of the funds;
- The date of determination;
- The name of the member of senior management who reviewed the transaction or approved keeping the account open; and
- The date the transaction was reviewed.

As a best practice, we should also record the nature of the relationship between the client and the PEP or HIO, as applicable.

5 List Screening

We screen our active customer base against publicly available lists of known terrorist individuals, such as the UNSC consolidated lists, the Consolidated Canadian Autonomous Sanctions List, the Public Safety Canada list, and the Canadian Sanctions Justice for Victims of Corrupt Foreign Officials Act.

Screening is conducted automatically at the time of onboarding and periodically throughout the relationship with the customer. Where there is a pending alert (possible match), the onboarding cannot be completed.

Potential matches are resolved by the Compliance Officer or a delegate. The investigation of a potential match may require us to obtain additional information or documentation from the customer.

In the event that a listing match is deemed to be a true match, the Compliance Officer will freeze the account and send reports to FINTRAC, CSIS, and the RCMP.

The Compliance Officer will develop messaging for staff in dealing with the customer to explain the freezing of the accounts and conduct an investigation to determine whether there are any other clients affiliated with the listed person or entity.

If our customer is not a listed person or entity, or we are not in possession of property belonging to the customer, an STR or ASTR should still be filed if there are reasonable grounds to suspect terrorist financing and/or terrorist activity.

Records of all investigations, including the rationale for match/no match decisions, must be maintained for at least five years.

6 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) and the Royal Canadian Mounted Police (RCMP)).
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.

7 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 change 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 can 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.

7.1 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.

7.2 Customers & Business Relationships That Are Not High Risks

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 Canada Pvt Ltd).

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 Canada Pvt Ltd. In such cases, a detailed rationale must be documented.

7.3 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 Canada Pvt Ltd 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 Canada Pvt Ltd 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 include 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 a 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 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 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.

7.4 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 is known to be involved in money laundering and/or terrorist financing-related activities;
- Any person or entity believed to be attempting to use Trackon Canada Pvt Ltd to conduct or be paid for illegal activities; and
- Any person or entity that has 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.