Trackon Canada Private Ltd

Anti-Money Laundering

&

Counter Terrorist Financing

Procedures for All Staff

Version Number: 1.1

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

1 Staff 4

2 Staff Procedure 4

3 Money Laundering & Terrorist Financing 4

3.1 How Money Laundering & Terrorist Financing Work 4

4 Customers 5

5 Customer Identification 6

5.1 Government Issued Photo Identification Method for Individuals 6

5.2 Other Identification Methods for Individuals 7

5.2.1 Single Process Method 8

5.2.2 Dual Process Method 8

5.3 Confirming Information for Organizations 10

5.3.1 Key Persons: Beneficial Owners & Directors 11

5.3.2 Key Persons: Signing Authorities 12

5.3.3 Confirming Existence, Address, Structure, Ownership & Signing Authority 12

5.4 Business Relationships 15

5.5 Customers That Cannot Be Identified 15

5.6 Records Related to "Reasonable Efforts" 15

6 Reporting 16

6.1 Suspicious Transactions & Attempted Suspicious Transactions 16

6.2 Electronic Funds Transfers Transactions 17

6.2.1 PEP & HIO Determinations 17

6.3 Terrorist Property 20

7 Responding to Law Enforcement Requests 20

8 Unusual Indicators & Red Flags 20

8.1 General 20

8.2 Knowledge of Reporting or Record Keeping Requirements 21

8.3 Identity Documents 22

8.4 Economic Purpose 22

8.5 Transactions Involving Areas Outside Canada 22

8.6 Remittance Transactions 23

8.7 Other MSB Transactions 23

8.8 Businesses That Send or Receive Electronic Funds Transfers (EFTs) 23

8.9 Indicators Specific to Human Trafficking 24

8.9.1 Types of Financial Transactions 25

8.9.2 Contextual Indicators 26

8.9.3 Know Your Customer 26

8.10 Indicators for Laundering the Proceeds of Fentanyl Trafficking 27

8.10.1 Procurement of Fentanyl via MSBs 27

8.10.2 Laundering the Proceeds of Low-level Drug Trafficking 27

8.11 Indicators for Laundering the Proceeds of Romance & Mass Marketing Fraud 28

8.11.1 Indicators relating to romance fraud victims 28

8.11.2 Indicators associated with transactions related to romance fraud 28

8.11.3 Indicators of mass marketing fraud 29

9 Appendix: Unusual Transaction Form (Internal) 30
9.1 Compliance Use Only 32

1 Staff

For the purposes of this document, references to staff and employees include any other third party companies (including subcontractors) that perform relevant functions including customer interactions, customer identification and transaction related functions.

All procedures listed in this document are mandatory. In addition to reading this document, all employees are required to complete training at least annually.

2 Staff Procedure

As a Money Services Business (MSB), we are required under Canadian legislation to have an anti-money laundering (AML) and counter terrorist financing (CTF) compliance program. This procedure should be read in conjunction with Trackon Canada Private Ltd (Trackon)'s Canadian AML & CTF Policy and Risk Assessment. Additional procedures applicable to compliance staff only are documented in a separate procedure.

This procedure has been designed to assist staff who deal directly with our customers and our transactions. We are required to verify, collect, and record information about our customers and transactions. Violations of this procedure can have severe negative consequences for Trackon. Any questions or concerns about this procedure should be directed to the Compliance Officer.

3 Money Laundering & Terrorist Financing

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

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

3.1 How Money Laundering & Terrorist Financing Work

Money laundering is described as having three phases by the Financial Action Task Force ('FATF'). These are 'Placement', 'Layering' and 'Integration'[1].

[1] http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

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

Placement: In the initial - or placement - stage of money laundering, the launderer introduces illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

Layering: After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

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

4 Customers

When customers initiate applicable transactions (described below), we must conduct identification measures before those transaction can be completed. In these cases, we collect identification information and information about the customer (individuals and organizations).

For customers where there is an existing customer record, we do not need to re-identify the customer at the time of a transaction if they are authenticated, and their identification information on file is up to date.

Periodically (based on risk level), customer information and identification (if applicable) is updated.

5 Customer Identification

In some cases, we need to identify our customers and record specific information about the customer. These situations are not negotiable. If we are not able to identify the customer, we must decline the following types of transactions as it applies to our business:

- Any customer, who is an entity, with whom we have an ongoing service agreement; and
- Electronic funds transfers valued at CAD 1,000 or more.

In other cases, we must attempt to identify the customer, if it is possible to do so, without letting the customer know that we may have suspicions about the nature of their activities. These include:

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

In cases that we cannot identify a customer, we must document the reasons that the customer could not be identified and our efforts to identify them. These customers will be considered higher risk and enhanced due diligence measures will be applied by the Compliance Officer. In some cases, the Compliance Officer may contact you to reach out to the customer for additional information.

5.1 Government Issued Photo Identification Method for Individuals

Trackon can confirm the identity of a customer, that is an individual, by relying on an identity document where it is "valid, authentic and current." Meaning, we can confirm identification using acceptable documents, presented in an electronic format, so long as it can be authenticated. The identification document must:

- Be issued by a provincial, territorial or federal government in Canada or an equivalent foreign government;
- Be valid (not expired);
- Bear a unique identifier number (such as a driver's license number);
- Bear the name of the individual being identified; and
- Bear a photo of the individual that we are identifying.

In many provinces and territories, the law prevents the use of health cards for use as non-health related identification. For this reason, we will not accept health cards as identification, without first referring the matter to the Compliance Officer.

We will specifically accept the following forms of photo identification:

- Driver's license;
- Passport;
- Provincial or territorial photo identification card with photo;
- Canadian Firearms Possession and Acquisition License (PAL);
- Canadian Citizenship Card with photo (issued before March 31, 2013);

- Canadian Permanent Resident Card with photo;
- Canadian Armed Forces Identification Card; or
- Secure Certificate of Indian Status (SCIS) with photo.

The Compliance Officer must approve any identification document that is not on the list that appears above before the customer will be considered to be identified.

We must also collect and record the following information:

- The customer's full name (no initials, short forms or abbreviations);
- The customer's occupation (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The customer's date of birth (if this appears on the identification document, the date of birth that we record must match the document);
- The customer's full home address (post boxes, office addresses and general delivery addresses are not acceptable for this purpose; if the customer wishes to provide a separate mailing address we can collect this as well, but we must always record the full home address);
- The place and country that the identification was issued;
- The unique identification number (such as the driver's license number);
- The expiry date of the identification provided (if the document has an expiry date; if it does not, please make a note to say that there was no expiry date on the document);
- The date on which we verified the document.

If a customer has been identified previously and the information in our records is up to date (the identification document used has not expired), and we recognize the customer (either by seeing them or hearing their voice), then we do not need to request identification to complete a transaction.

We determine the authenticity of a government-issued photo identification document and verify it matches our customer by using a software platform called ShuftiPro[2]. The software connects via API where our customers present their ID and follow the prompts to provide a facial capture which incorporates liveness testing. Certain data is extracted automatically from the ID using Optical Character Recognition (OCR). The ID image is also used to verify the authenticity of the document by matching certain characteristics, such as the security features, the text format and the spacing. Using facial recognition software, ShuftiPro compares the image on the ID with the liveness video uploaded by the customer. Trackon is provided with a pass or fail result.

5.2 Other Identification Methods for Individuals

We can also use the following methods to identify our customers that are individuals.

[2] https://shuftipro.com/

5.2.1 Single Process Method

We may confirm the identity of a client by referring to their Canadian credit file (Equifax or TransUnion), provided it has been in existence for at least three years, by doing a credit header match. Meaning, we do not have to collect a credit assessment (hard hit) but simply a credit header match (soft hit). This must be completed at the time we are confirming our client's identity. To be acceptable, the credit file details must match the name, date of birth and address provided by the client. If any of the information does not match, we will need to use the dual process method to confirm the client's identification.

When using this method to confirm our client's identity, we must record the following information:

- The client's name;
- The name of the Canadian credit bureau holding the credit file (Equifax or Transunion);
- The reference number of the credit file; and
- The date we consulted the credit file.

Trackon does not currently use this method for identification. We have included this for educational purposes.

5.2.2 Dual Process Method

Where the single process method provides information that does not match what the client has provided us, or the credit file has not been in existence for the required three (3) years, we must use the dual process method. This involves referring to information from reliable and independent sources, and must be valid and the most recent. In order to qualify as reliable, the sources should be well known and considered reputable.

Independent means the sources providing the information cannot be us (as the reporting entity) or the client, and the documents referred to cannot be from the same source. For example, reliable and independent sources can be the federal, provincial, territorial, and municipal levels of government, crown corporations, financial entities, or utility providers.

Under the dual process method, we can refer to any two of the following options:

- Documents or information from a reliable source that contain the client's name and address;
- Documents or information from a reliable source that contain the client's name and date of birth; or
- Documents or information that contain the client's name and confirms that they have a deposit, credit card or other loan account with a financial entity.

The table below provides examples of the sources and documents that can be referred to when confirming a client identification. In order to meet the standards

of the dual process method, we must rely on two documents provided by the client, but each document referred to cannot be in the same column.

Documents or information to verify name and address **Column A**	**Documents or information to verify name and date of birth** **Column B**	**Documents or information to verify name and confirm a financial account** **Column C**
Issued by a Canadian government body: Any card or statement issued by a Canadian government body (federal, provincial, territorial, or municipal): • Canada Pension Plan (CPP) statement; • Property tax assessment issued by a municipality; or • Provincially-issued vehicle registration. Benefits statement • Federal, provincial, territorial, and municipal levels. CRA documents: • Notice of assessment; • Requirement to pay notice; • Installment reminder/receipt; • GST refund letter; or • Benefits statement.	Issued by a Canadian government body: Any card or statement issued by a Canadian government body (federal, provincial, territorial, or municipal) • Canada Pension Plan (CPP) statement of contributions; • Original birth certificate; • Marriage certificate or government-issued proof of marriage document (long-form which includes date of birth); • Divorce documentation; • A permanent resident card; • Citizenship certificate; or • Temporary driver's license (non-photo).	Confirm that your client has a deposit account, credit card or loan account by means of: • Credit card statement; • Bank statement; • Loan account statement (for example: mortgage); • Cheque that has been processed by a financial institution; • Telephone call, email or letter from the financial entity holding the deposit account, credit card or loan account; • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months); or • Use of micro-deposits to confirm account.
Issued by other Canadian sources: • Referring to the client's Canadian credit file that has been in existence for at least 6 months; • Utility bill (for example, electricity, water, telecommunications); • T4 statement; • Record of Employment; • Investment account statements (for example,	Issued by other Canadian sources: • Referring to a client's Canadian credit file that has been in existence for at least 6 months; • Insurance documents (home, auto, life); or • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months).	

Documents or information to verify name and address Column A	Documents or information to verify name and date of birth Column B	Documents or information to verify name and confirm a financial account Column C
RRSP, GIC); or • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months).		
Issued by a foreign government: • Travel Visa.		

Where we use the dual process method to confirm the identity of a client, we must record certain information. Specifically:

- The client's name;
- The name of the two different sources that were used to identify our client;
- The type of information (for example, utility statement, bank statement, marriage license, CRA notice of assessment, etc.) that was referred to;
- The account number associated with the information;
- If there is no account number, you must record a reference number that is associated with the information; and
- The date we verified the information.

Where a customer is not identified using the Government-Issued Photo ID method, Trackon may request documentation under the dual process method be submitted for review. This will be a manual process where the Compliance Officer must provide approval before any transactions take place.

5.3 Confirming Information for Organizations

If the customer is an organization (such as a company, partnership or charitable foundation) then we need to collect and record information about the organization, as well as obtain documentation that includes:

- Their full legal name (no initials, short forms or abbreviations);
- The organization's structure (incorporated company, trust, partnership, etc.);
- The organization's "principal business" (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The organization's physical address (post office boxes and general delivery addresses are not acceptable for this purpose; if the customer wishes to

provide a separate mailing address, we can collect this as well, but we must always record their physical address);
- The organization's telephone number;
- A list of Directors; and
- Information about the organization's beneficial owners.

Additional information based on the type of organization:

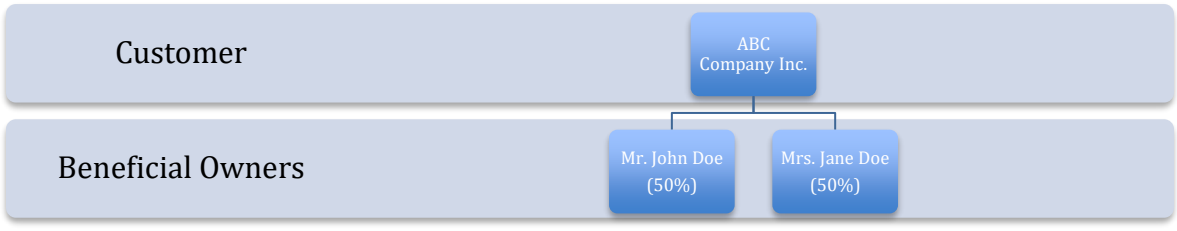
Incorporated Company	Not-For-Profit Organizations
Incorporation Number Place of Incorporation	Whether the organization solicits donations from the public. If donations are solicited, whether or not the organization is a registered charity in Canada. If the organization is a registered charity, their registration number.

5.3.1 Key Persons: Beneficial Owners & Directors

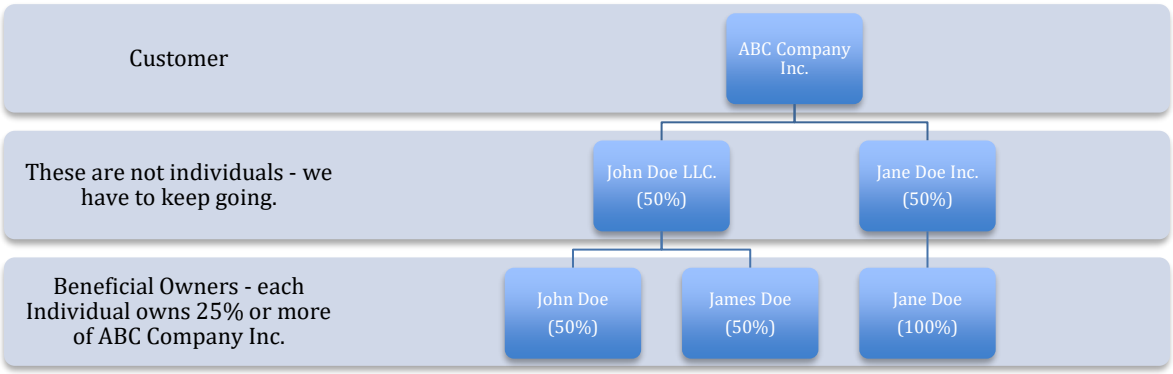
We must collect information about an organization's beneficial owners. Who is a beneficial owner will depend on the type of organization.

Incorporated Company or Partnership	Trusts	Other Organizations
All Directors and individuals who own or control, directly or indirectly, 25 percent (%) or more of the organization.	All trustees and all known beneficiaries and settlors of the trust.	All individuals who own or control, directly or indirectly, 25 percent (%) or more of the organization.

Direct Beneficial Ownership (Example):



Indirect Beneficial Ownership (Example):



We must collect the following information about all beneficial owners of an organization:

- Their full legal name (no initials, short forms or abbreviations);
- Their full home address[3] (post office boxes, business offices and general delivery addresses are not acceptable for this purpose); and
- Their role and/or ownership stake in the organization.

We must collect the following information about all directors of an organization:

- Their full legal name (no initials, short forms or abbreviations).

5.3.2 Key Persons: Signing Authorities

A signing authority is a person that has the authority to act (sign) on behalf of the organization. We must identify at least one signing authority for each organization (this is done using the same methods used to identify individuals). When identifying a signing authority, we must be sure to collect and record:

- Their full legal name (no initials, short forms or abbreviations);
- Their full home address[4] (post office boxes, business offices and general delivery addresses are not acceptable for this purpose); and
- Their role and/or ownership stake in the organization.

If there are more than three signing authorities, we are only required to identify three (not all) signing authorities.

5.3.3 Confirming Existence, Address, Structure, Ownership & Signing Authority

In addition to collecting information about our customers that are entities, we must confirm that this information is accurate. We will, where possible, attempt to confirm this information electronically. Where such confirmation is not possible, we

---

[3] If the individual is not a resident of Canada, the address that we collect must be their foreign permanent address.

[4] If the signing authority is not a resident of Canada, the address that we collect must be their foreign permanent address.

will request that the organization provide documentation to confirm the information that was given.

Organization Type	Existence & Structure	Address (only if not confirmed by Existence & Structure documents)	Ownership (only if not confirmed by Existence & Structure documents)	Signing Authority (only if not confirmed by Existence & Structure documents)
Incorporated Company	-Articles of Incorporation -Certificate of Incorporation -Tax document or communication from Canada Revenue Agency (CRA) -Business License	-Utility bill from a recognized provider (phone, internet, etc.) -Statement or communication from recognized Canadian financial institution or insurance company - Tax document or communication from CRA - Correspondence from a Canadian government or government organization (federal or provincial)	-Articles of Incorporation and/or Amendment (where shareholders are listed) -Shareholder registry -CRA Schedule 50 -Share Certificates	-Articles of Incorporation and/or Amendment (where signing authorities are listed) -Resolution by the Board of Directors -Attestation
Partnership	-Partnership Agreement -Tax document or communication from CRA -Business License		-Partnership Agreement and/or Amendment (where partners are listed) -Partner registry	-Partnership Agreement and/or Amendment (where signing authorities are listed) -Resolution by the Board of Directors -Attestation
Not-For-Profit/Charity	-Articles of Association -Tax document or communication from CRA		-Articles of Association and/or Amendment -Ratified meeting minutes listing all directors	-Resolution by the Board of Directors -Trust Charter -Trust Ledger
Trust	-Trust Charter -Trust Ledger		-Trust Charter -Trust Ledger	-Trust Charter -Trust Ledger

Organization Type	Existence & Structure	Address (only if not confirmed by Existence & Structure documents)	Ownership (only if not confirmed by Existence & Structure documents)	Signing Authority (only if not confirmed by Existence & Structure documents)
Informal Organization	-Board resolutions; or -Meeting minutes -Official attestation from the organization's leadership.		-Ratified meeting minutes listing all controlling persons -Attestation	Ratified meeting minutes listing all signing authorities -Attestation

If information about the organization, such as the ownership structure, cannot be confirmed, the Compliance Officer is notified and the organization is considered to be high risk and subject to enhanced due diligence (EDD). At the Compliance Officer's discretion, the organization may be considered outside of our risk tolerance.

Where a customer is considered to be high risk, EDD measures are applied. In some cases, this will require the collection of additional documentation and/or information from the customer, including taking reasonable measures to verify the identity of the most senior managing officer of the entity.

The information that you collect about an organization does not require original documents. It can be sent to us by mail, email, or online upload if the person requesting the transaction needs to get information that they don't have on hand at the time. If it has been more than a year since we collected any information about an organization we will ask the customer, at the time of their next transaction, whether the structure, control or the ownership of the organization has changed, and record the answers provided by the customer.

At the point that we onboard an organization, we must also consult our policies regarding prohibited industries to ensure that the organization's business type is within our risk tolerance. If an organization's business type is outside of our risk tolerance, the IT system will not allow the organization to proceed.

Organizations must upload all supporting documentation electronically. This information is verified manually by staff and approved by the Compliance Officer before any transactions can be performed. Any issues or concerns with verification of information is escalated to the Compliance Officer or a designate.

5.4 Business Relationships

We have a business relationship with any individual customer that has completed two or more transactions that require us to identify the customer (refer to the customer identification section above). We also have a business relationship with any customer with whom we have entered into an ongoing service agreement, which includes all customers that are organizations. In these cases, we must ask about the purpose of the customer's business relationship with us and record that purpose. In most cases, this will be relatively straightforward, for example "sending money to family." The answers that we record should be as specific as possible.

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.

5.5 Customers That Cannot Be Identified

If we are not able to identify a customer, we will not accept that customer.

Some customers may be hesitant to provide identification for legitimate reasons. Remember that if you are obtaining identification because you suspect that the customer's transactions or requests are related to terrorist financing or money laundering, you should not tell the customer about your suspicion. Instead, let the customer know that it is our company's policy to ask for identification. Since most objections will be related to privacy and marketing, and not AML or CTF, let the customer know that the information will not be used for marketing purposes if they do not wish to receive marketing messages from Trackon[5].

5.6 Records Related to "Reasonable Efforts"

In any case where Trackon is required to take reasonable efforts to obtain or confirm information and/or collect documentation, we must keep a record of those efforts, whether or not they are successful and the date the reasonable measures were taken.

For example, in the case that a potential customer quickly changes their mind about completing a transaction when he or she is asked to provide identification documents, Trackon would be required to report an ASTR. In this case, the reasonable effort to identify the person was to ask them for identification documents, which they refused to provide. We would keep a record of this information and include it in the ASTR that we file with FINTRAC.

These records are maintained electronically.

---

[5] If the customer indicates that they do not wish to receive marketing messages, this should be noted and passed on to the Privacy Officer to be certain that the customer is not added to marketing lists.

6 Reporting

Trackon must report certain types of transactions.

Reporting to any regulatory, law enforcement, or government agency should always be completed by the Compliance Officer or a designate (a person that has been trained to submit reports in the Compliance Officer's absence).

All other employees should use the internal forms included in this program (i.e. Unusual Transaction Form) to submit reports to the Compliance Officer.

If you aren't sure whether or not you will need to submit a report, speak with the Compliance Officer for clarification. If it is not possible to speak with the Compliance Officer at that time, err on the side of caution by collecting the information that you need to fill out the form(s) and submit the report(s).

This may include collecting the customer's identification information.

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

These transactions are detected automatically by the IT system and escalated manually by staff members. The Compliance Officer reviews transaction related alerts on a regular basis.

6.1 Suspicious Transactions & Attempted Suspicious Transactions

Suspicious Transaction Reports (STRs) and Attempted Suspicious Transaction Reports (ASTRs) are submitted to FINTRAC where there are reasonable grounds to suspect that an activity is related to money laundering or terrorist financing. These reports must be submitted whether or not the transaction or activity is completed.

However, our staff will apply a lower threshold for escalation to the Compliance Officer, which is suspicion. Suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a "gut feeling" or "hunch". In other words, if you have a feeling that something is unusual or suspicious, but do not have any facts, context, or indicators to support that feeling or to reasonably conclude that an ML/TF offence has occurred, escalate it to the Compliance Officer for determination.

ASTRs are used for transactions that are not completed, whether the transaction is declined by Trackon or cancelled by the customer.

Employees should report this type of transaction using the Unusual Transaction Form (Internal), contained in an appendix. A list of suspicious transaction indicators is also included in this document and should be reviewed regularly by all staff.

It is important not to let the customer know that you are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. You are,

however, protected under Canadian law from any action when you submit a report in good faith. In most cases, even when a case goes to court, the customer will not know that this report has been filed.

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

STRs and ASTRs must be submitted to FINTRAC as soon as practicable after we have taken measures that enable us to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist activity financing offence. In order to meet our obligations, the internal form must be submitted to the Compliance Officer on the same day that the transaction occurs.

6.2 Electronic Funds Transfers Transactions

Electronic Funds Transfer Reports (EFTRs) are submitted when a customer requests the sending of funds into or out of Canada valued at CAD 10,000 or more. This may be in a single transaction, or several separate transactions in the same 24-hour period.

EFTRs must be submitted to FINTRAC within 5 working days; in order to provide enough time for the Compliance Officer to complete reporting, the internal form must be submitted on the same day that the transaction occurs.

6.2.1 PEP & HIO Determinations

Currently, in the case of EFTs for amounts valued at CAD 100,000 or more, we must also determine whether or not the customer is a Politically Exposed Person (PEP) or Head of an International Organization (HIO). As of June 1, 2021, MSBs will be required to do Politically Exposed Person (PEP) checks when we enter into a business relationship with a 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).

Foreign PEPs are people who hold or have ever held any of these positions on behalf of a foreign government:

- 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 counsellor 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 court of last resort;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

Domestic PEPs are people who hold or have ever held any of these positions on behalf of the federal government or a provincial/territorial 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 counsellor 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.

Domestic PEPs also include 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
- 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 own or control 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 a 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 an Trackon employee becomes aware that our customer is a PEFP, PEP, or HIO, they will notify the Compliance Officer immediately so that a risk assessment can be performed, and an adjustment can be made to the client's risk rating. Foreign PEPs, their family members and close associates are automatically considered high risk customers.

In the event that a customer is determined to be a PEFP, 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 PEFP determination.

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

- Office or position of the PEP or HIO;
- Name of the organization or institution of the PEP or HIO;
- Source of the funds;
- Source of wealth;
- Date of determination;
- Name of the member of Senior Management who reviewed the transaction or approved keeping the account open; and
- Date the transaction was reviewed.

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

The Compliance Officer must be notified immediately when a customer is a PEP. The Compliance Officer will review the transaction and provide sign-off on behalf of Senior Management. This sign-off must be recorded within 30 calendar days of the date that we determine that our customer is a PEP.

6.3 Terrorist Property

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

These reports should be escalated to the Compliance Officer immediately. In some cases, property or funds must be frozen.

Like STRs and ASTRs, the contents of these reports, or the fact that you are filing a report, should not be disclosed to the customer.

TPRs must be submitted to FINTRAC and other agencies immediately. In order to provide enough time for the Compliance Officer to complete reporting, the internal form must be submitted on the same day that the transaction occurs.

7 Responding to Law Enforcement Requests

If staff are aware that a request has been made by law enforcement, they must immediately notify the Compliance Officer who will handle all related correspondence.

8 Unusual Indicators & Red Flags

There are a wide variety of indicators that can let us know that a transaction or request may be related to money laundering or terrorist financing. These include customer behaviours, as well as transaction patterns. Trust your instincts – if something doesn't feel right (whether or not any of these indicators are present), file an Unusual Transaction Report with the Compliance Officer.

These indicators are a sample provided by FINTRAC and will be augmented regularly by the Compliance Officer based on trends that we have observed in our business transactions and/or industry.

8.1 General

- The individual or entity appears on a government sanctions list.
- Customer admits or makes statements about involvement in criminal activities.
- Customer shows uncommon curiosity about internal systems, controls, and policies.
- Customer has only vague knowledge of the amount of a transaction.

- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer over justifies or explains the transaction.
- Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account.
- Normal attempts to verify the background of a new or prospective customer are difficult.
- Customer appears to be acting on behalf of a third party, but does not tell you.
- Customer is involved in activity out-of-keeping for that individual or business.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the customer's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the customer.
- Customer attempts to develop close rapport with staff.
- Customer spells his or her name differently from one transaction to another.
- Customer provides false information or information that you believe is unreliable.
- Customer offers you money, gratuities, or unusual favours, for the provision of services that may appear unusual or suspicious.
- You are aware that a customer is the subject of a money laundering or terrorist financing investigation.
- You are aware or you become aware from a reliable source (that can include media or other open sources) that a customer is suspected of being involved in illegal activity.
- You know a new or prospective customer as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

8.2 Knowledge of Reporting or Record Keeping Requirements

- Customer attempts to convince employee not to complete any documentation required for the transaction.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer seems very conversant with money laundering or terrorist activity financing issues.
- Customer is quick to volunteer that funds are “clean” or “not being laundered.”

- Customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds.
- Customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds.

8.3 Identity Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only submits copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details such as a phone number.
- Customer inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Customer presents different identification documents at different times.
- Customer alters the transaction after being asked for identity documents.
- Customer presents different identification documents each time a transaction is conducted.

8.4 Economic Purpose

- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the customer.
- Activity is inconsistent with what would be expected from declared business.
- A business customer refuses to provide information to qualify for a business discount.
- No business explanation for size of transactions or cash volumes.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

8.5 Transactions Involving Areas Outside Canada

- Customer and other parties to the transaction have no apparent ties to Canada.
- International remittances in excess of average income for migrant worker customers.
- Excessive demand for migrant remittances from individuals or entities based on migrant worker population.
- Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.

- Transaction involves a country known for highly secretive banking and corporate law.
- Transactions involving any countries deemed by the Financial Action Task Force as requiring enhanced surveillance.
- Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transactions followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
- Transaction involves a country known or suspected to facilitate money laundering activities.

8.6 Remittance Transactions

- Customer shows unusual interest in funds transfer systems and questions the limit of what amount can be transferred.
- Size of funds transfers is inconsistent with normal business transactions for that customer.
- A customer sends or receives multiple transfers to or from the same individual.
- Migrant remittances made outside the usual remittance corridors.
- Country of destination for a transfer is not a member of the Financial Action Task Force or an FATF Style Regional Body. To find out which countries are members of the FATF, refer to its Web site (http://www.fatf-gafi.org).
- Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices.

8.7 Other MSB Transactions

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer wants to pay transaction fees that exceed the posted fees.
- Customer enters into transactions with counter parties in locations that are unusual for the customer.

8.8 Businesses That Send or Receive Electronic Funds Transfers (EFTs)

- Customer is reluctant to give an explanation for the remittance.
- Customer orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Customer instructs you to transfer funds abroad and to expect an equal incoming transfer.

- Customer shows unusual interest in funds transfer systems and questions the limit of what amount can be transferred.
- Customer sends frequent wire transfers to foreign countries, but does not seem to have connection to such countries.
- Size of funds transfers is inconsistent with normal transactions for that customer.
- Several customers request transfers either on the same day or over a period of two to three days to the same recipient.
- Several customers requesting transfers share common identifiers, such as family name, address or telephone number.
- Several different customers send transfers that are similar in amounts, sender names, and destination country.
- A customer sends or receives multiple transfers to or from the same individual.
- Stated occupation of the customer or the customer's financial standing is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).
- Migrant remittances made outside the usual remittance corridors.
- Country of destination for a wire transfer is not consistent with the nationality of the individual customer.
- Customer requests transfers to a large number of recipients outside Canada who do not appear to be family members.
- Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.
- Customer makes funds transfers to free trade zones that are not in line with the customer's business.
- Country of destination for a transfer is not a member of the Financial Action Task Force or an FATF Style Regional Body.
- Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices.

8.9 Indicators Specific to Human Trafficking

The following indicators are specific to human trafficking for sexual exploitation and reflect types and patterns of transactions, contextual factors and those that emphasize the importance of knowing your customer. These indicators and other facts surrounding a financial transaction should be considered as a whole. This is important because a single transaction taken in isolation may lead to a false assumption of normalcy. Considering all indicators may reveal otherwise unknown links that taken together could lead to reasonable grounds to suspect that the transaction consists of proceeds from human trafficking.

8.9.1 Types of Financial Transactions

- Online advertising and promotional services (e.g. escort services, massage services, relationship services, related peer-to-peer online booking services): frequent payments in multiples of small amounts (e.g. $3, $12, $24) in relatively short timelines and inconsistent with expected activity;
- Accommodations (e.g. hotels, motels, peer-to-peer online booking services for private and commercial lodgings): payments for short stays and/or stays in multiple cities in a relatively short time period;
- Distance transportation: frequent purchases for airline, train, and/or bus tickets, possibly for multiple individuals, in relatively short timelines and inconsistent with expected activity;
- Local transportation: purchases for taxi, limousine, vehicle rentals, and ride sharing services in relatively short timelines and inconsistent with expected activity;
- Fast food restaurants: frequent low value purchases in relatively short timelines and inconsistent with expected activity;
- Drug stores, clothing stores, beauty stores (e.g. lingerie, make-up): frequent purchases in relatively short timelines and inconsistent with expected activity;
- Strip clubs, massage parlors, beauty salons and modelling agencies: credit card payments for purchases made after the establishments' normal hours of business;
- Bitcoins or other virtual currencies: frequent purchases in multiples of small amounts (e.g. $3, $12, $24), directly by the customer or through exchanges;
- Online payment services companies: personal account activity inconsistent with expectations involving frequent deposits and payments through an online payment service in small amounts typically under $100. Account funds may then be used for virtual currency deposits/redemptions, or payment of bills, such as personal or third party credit cards;
- Rent payments: for addresses where prostitution is reported to occur by media, law enforcement, or classified ads; and,
- Credit card purchases: for online purchases which provide relative anonymity.
- Patterns of Financial Transactions and Account Activity
- Cash deposits/withdrawals between the hours of 10 p.m. and 6 a.m.;
- Multiple cash deposits conducted at different bank branches/ATMs, possibly across different cities and provinces;
- Frequent transactions (e.g. purchases, payments, account debits/credits, electronic transfers) across different cities and provinces within short timelines;
- Multiple deposits and/or incoming email money transfers or other forms of electronic transfers, possibly using a temporary address (e.g. hotel), from unrelated third parties with little or no explanation;
- Account funded primarily via third party cash transactions;

- Deposits (e.g. via ABM, in-branch, email money transfers, other forms of electronic transfers) followed rapidly by cash withdrawals, bill payments, and/or electronic transfers;
- Personal account receives frequent deposits but is typically kept depleted, showing no purchases or transactions that would indicate normal activity;
- Account appears to function as a funnel account; deposits occur in locations where the customer does not reside or conduct business;
- Deposits (e.g. via ABM, in-branch) conducted in one city followed by same day or next day withdrawal and/or purchase conducted in another city;
- Unrelated third parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient or no stated purpose for the transfers;
- Email money transfers to third parties with alternate names provided in brackets [e.g. jane@example.com (Bambi)];
- Large and frequent electronic transfers between senders and receivers with no apparent relationship;
- Common address provided by different people undertaking domestic/international funds transfers;
- Rounded sum hotel transactions;
- Hotel transactions by the same individual for two separate rooms for the same dates;
- Hotel transactions followed by a refund for the same amount; and,
- Pre-authorized hotel by credit card, but accommodations are actually paid for using cash.

8.9.2 Contextual Indicators

- Media or other reliable sources suggest that a customer may be linked to criminal activity which could generate proceeds of crime;
- Media coverage of account holder's activities relating to human trafficking in the sex trade and/or prostitution rings;
- Use of addresses where prostitution is reported to occur by media, law enforcement, or classified ads;
- Phone number provided on online advertising and promotional services is used in different cities and provinces in a short period of time;
- Use of a third party to execute transactions (for example, under the pretext of requiring an interpreter); and,
- Customer makes deposits accompanied or watched by a third party who may, on separate occasions, accompany or watch customers who are making deposits. The third party may be handing over to the customer what is subsequently confirmed to be the customer's identification.

8.9.3 Know Your Customer

- Financial activity is inconsistent with that expected based on one or more of the following: the customer's financial status, stated occupation, type of account or stated business activity;

- Customers give contact/identifying information that is traceable through open sources to advertising related to escort services;
- Use of someone else's identification, or opening an account in the name of an unqualified minor;
- Use of aliases for the purpose of opening multiple accounts in different banks, or in different branches of the same bank; and,
- Addition of an unusual number of individuals as joint account holders, or authorized users to products such as credit cards.

8.10 Indicators for Laundering the Proceeds of Fentanyl Trafficking

Trackon considers the following indicators relevant to their sector in tandem with the low-level drug trafficking indicators that follow to effectively identify potential money laundering activities associated with the trafficking of fentanyl.

8.10.1 Procurement of Fentanyl via MSBs

- Customer purchases wire transfers or money orders for amounts below the $10,000 reporting threshold at multiple money services businesses over a short time period, normally with cash or prepaid credit cards. Typically, the wire transfers and money orders are sent by numerous, seemingly unconnected individuals in Canada to the identical recipients in China (in Wuhan, Zhuhai, Guangzhou, Xianju and Shanghai, in particular), Ukraine and India.
- Customer pays for wire transfers in Canadian funds, which are then received in even dollar amounts.
- Customer sometimes uses a post office box as a mailing address.
- Customer receives multiple direct deposits from global payment processing and/or virtual currency exchange platforms, typically in amounts below the reporting threshold.
- Customer requests wire transfers to companies advertising the sale of fentanyl and/or its known chemical precursors: NPP (1-Phenethyl-4-piperidone); ANPP (4-azido-2-nitrophenyl Phosphate) and Norfentanyl (N-phenyl-N-pieridin-4ylpropanamide).

8.10.2 Laundering the Proceeds of Low-level Drug Trafficking

- Customer makes transactions that are inconsistent with his or her employment or profile.
- Customer conducts untypical cash transactions given his or her profile.
- Customer makes ATM transactions for larger amounts than would normally be expected.
- Customer lives beyond his or her apparent means, as evidenced by large credit card or other bills, or expenses for real estate or luxury goods.
- Customer incurs significant travel expenses that are inconsistent with his or her profile, such as for car rentals, hotel bills, airline tickets and gasoline.

- Customer has funds deposited into his or her account in amounts below the reporting threshold from what appear to be multiple third parties located in many parts of the city, a broader geographic area or several provinces.
- Customer is involved in financial transactions that have been the subject of negative media (stories about drugs and weapons offences).
- Customer uses multiple financial institutions; his or her account sees significant cash flow-through; and he or she carries out little typical banking activity (such as paying household bills).
- Customer is a commercial entity that engages in trade transactions for products that do not appear to fit its known business profile.

8.11 Indicators for Laundering the Proceeds of Romance & Mass Marketing Fraud

Trackon considers the following indicators that follow to effectively identify potential money laundering activities associated with romance and mass marketing fraud.

8.11.1 Indicators relating to romance fraud victims

- Customer met the individual they are transacting with on a social media platform, via email or on a dating website.
- Customer always, or almost always, communicates with the individual they met online by email or text.
- Customer has never met or has never seen the individual they are in the relationship with, and is often older than that individual.
- Customer relays a confusing, conflicting or non-believable story about why the funds are needed or the transaction is taking place.
- Customer is at a potentially more vulnerable stage of life (i.e., a senior or widowed, separated or divorced).
- Customer provides minimal or inconsistent information and/or avoids answering questions about the purpose of the transaction.

8.11.2 Indicators associated with transactions related to romance fraud

- Customer appears to be pooling all financial resources from various sources (e.g., credit cards, loans, retirement savings, insurance policies) and depleting assets (e.g., home, vehicle, investments and retirement savings) to fund transfers to individuals/entities.
- Customer sends funds to another individual, and the amount or frequency of funds sent increases over time.
- Customer is transacting with one or more individuals suspected of being either a victim or perpetrator of romance fraud.
- Customer is identified as a victim and is transacting with one or more individuals who are also identified as victims of romance fraud.
- Customer either cancels transaction for no apparent reason or transaction is refused due to questionable rationale for it.

- Customer makes payments to online dating services or social media websites.
- Customer conducts large volume and/or excessive number of transactions involving foreign jurisdictions over a short period.
- Customer receives funds from numerous individuals in multiple jurisdictions. The funds are then depleted by cash withdrawals conducted in Canada or abroad, or by wires to the benefit of individuals/entities in Canada or abroad.

8.11.3 Indicators of mass marketing fraud

- Customer conducts financial activity or holds accounts at multiple financial entities without adequate rationale.
- Non-account holders or apparently unrelated individuals make deposits or payments to customer's account.
- Customer does not appear to know the sender of a wire transfer from whom the wire transfer was received, or the recipient to whom they are sending a wire transfer.
- Customer conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Account is used for pass-through activities (e.g. to receive and subsequently send funds to beneficiaries).
- Customer becomes defensive when asked about the rationale for a transaction and may take steps to close account or conduct transaction elsewhere.
- Customer orders wire transfers that are frequently returned or cancelled.
- Customer frequently deposits fraudulent cheques or bank drafts that are later returned by the financial institution.
- Customer appears to be directed by a third-party to deposit funds into accounts or to wire funds to individuals domestically or in foreign jurisdictions.
- Customer sends and/or receives an increasing amount of wires/EMTs.
- Customer's wire transfers involve amounts or jurisdictions that are inconsistent with their profile.
- Customer receives multiple incoming wires into a business account in a manner inconsistent with day-to-day business.
- Customer makes numerous third-party cash deposits followed by outgoing draft/wire transfers to or cash withdrawals in high risk jurisdictions.
- Customer receives payments from payment processors that are inconsistent with the customer's profile.

9 Appendix: Unusual Transaction Form (Internal)

This form should be completed if you have reasonable grounds to suspect that a customer's activities are related to money laundering or terrorist financing activities. This form should be submitted to the Compliance Officer on the same day that it is completed.

Do not let the customer know that you are filling out this form or discuss its contents with anyone other than the Compliance Officer or a designate.

Your Name & Location (Trackon Office Location):

_____

Customer's Name:

_____

Were you able to identify the customer?

If yes, please include the customer's identification information in the section below. If not, please explain why this was not possible (please use additional pages as needed):

_____

_____

_____

_____

Describe the customer's request or transaction, including whether the transaction was completed or not (please use additional pages as needed):

_____

_____

Describe in your own words what happened, and what made you suspicious. Please be as detailed as possible, and include facts about the customer's behavior, and any specific words or phrases that they used. Describe what you did and said, as well as how the customer responded. Please use additional pages as needed:

Date:

Time:

Your Signature:

9.1 Compliance Use Only

Date reviewed: _____

Reviewed By: _____

This transaction has been deemed suspicious: ____ Yes ____ No

Describe the rationale for the decision above (whether or not the transaction is deemed to be suspicious). Please use additional pages if required.

_____

_____

_____

_____

Describe any follow up actions (if applicable). For example, adjustments to the customer's risk rating, enhanced due diligence activities, etc.

_____

_____

_____