SECTION 18 REGULATIONS REGARDING THE PROCEEDS OF CRIME

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA"), mandates that all financial institutions report certain financial transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) - Canada's financial intelligence unit, which collects, analyzes and discloses financial information and intelligence on suspected money laundering and terrorist activities financing.

Definitions

Money Laundering is the process whereby 'dirty money', produced through criminal activity, is transformed into 'clean money' whose criminal origin is difficult to trace. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Under Canadian law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence, such as illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeiting, stock manipulation, etc.

Money laundering offences may also extend to property or proceeds derived from illegal activities that took place outside Canada.

Terrorist Financing may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Terrorist Property is defined as property in one's possession or control that is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property. "Property" is inclusive of any type of real or personal property, such as any deed or instrument giving title or right to property, or giving right to money or goods (i.e. money orders, real estate, mutual funds, and traveler's cheques). A terrorist or terrorist group can be a person, a group, a trust, a partnership, a fund, an unincorporated association or an organization.

If you know, or even if you suspect, that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, you should NOT complete the transaction. This is because terrorist property must be frozen under the United Nations Suppression of Terrorism Regulations as well as the Criminal Code.

Large Cash Transactions refer to a cash value of $10,000 or more Canadian dollars or its equivalent in foreign currency. All references to cash mean money in circulation, including bank notes or coins, and exclude personal or business cheques, money orders, or other similar negotiable instruments.

Methods of money laundering

There are many known methods to launder money and more are being devised every day. The methods are becoming more sophisticated and complicated as technology advances. Some of the most common methods are:

- **Nominees** - use of family members, friends, or associates who are trusted within the community and who will not attract attention. This facilitates the concealment of the source and ownership of the funds involved.

- **Structuring (smurfing)** - inconspicuous individuals deposit cash, buy bank drafts, or money orders at various institutions, usually for amounts less than the thresholds for reporting. The drafts or money orders are usually made payable to other parties and, along with cash, are typically deposited to a central account.

- **Bulk cash asset purchases** - individuals buy big-ticket items like cars, boats, and real estate for cash. Often these will be registered in other names to distance the launderer. The assets can then be sold and converted back to 'clean' cash.

- **Currency smuggling** - funds are moved across borders to other countries to disguise the true source and ownership of the funds. They are typically taken to countries where there are few, if any, laws to record the ownership of funds entering the financial system. These countries tend to also be those with very strict bank secrecy laws. Methods for smuggling include mail, courier, and body packing.

- **Exchange transactions** - proceeds of crime are used to buy foreign currency that can then be transferred to offshore bank accounts or converted back to functional currency at another institution.

- **Casino gambling** - individuals bring cash into a casino and buy casino chips/ tokens. After gaming and placing a few small bets, they redeem the remainder of the chips/tokens and request a casino cheque (often made payable to a third party).

- **Black market peso exchange** - this is a method primarily affecting the United States although Canada is not immune to it. There is an underground network of currency brokers who buy the US and Canadian dollars from the criminal and give them pesos. The brokers then sell these US and Canadian dollars to foreign companies for pesos who use the funds to purchase goods in the US and Canada for sale back home.

Methods of terrorist activity financing

There are two primary sources of financing for terrorist activities. The first involves getting financial support from countries, organizations, or individuals. The other involves revenue-generating activities.

- **Financial support** - Terrorism could be sponsored by a country or government, although this is believed to have declined in recent years. State support may be replaced by support from other sources, such as individuals with sufficient financial means. This could include, for example, donations to certain organizations that are known to have links to terrorists or terrorist groups.
- **Revenue-generating activities** - The revenue-generating activities of terrorist groups may include criminal acts, and therefore may appear similar to other criminal organizations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.

  Financing for terrorist groups may also include legitimately earned income, which might include collection of membership dues and subscriptions, sale of publications, speaking tours, cultural and social events, as well as solicitation and appeals within the community. This fundraising might be in the name of organizations with charitable or relief status, so that donors are led to believe they are giving to a legitimate good cause. Only a few non-profit organizations or supposedly charitable organizations have been implicated in terrorist financing networks in the past worldwide. In these cases, the organizations may in fact have carried out some of the charitable or relief work. Members or donors may have had no idea that a portion of funds raised by the charity was being diverted to terrorist activities. This type of "legitimately earned" financing might also include donations by terrorist group members of a portion of their personal earnings.

  The methods used by terrorist groups to generate funds from illegal sources are often very similar to those used by "traditional" criminal organizations. Like criminal organizations, they have to find ways to launder these illicit funds to be able to use them without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering. Therefore, a robust comprehensive anti-money laundering regime is key to providing the information necessary to identify and track terrorists' financial activities.

  Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

Politically Exposed Persons

A Politically Exposed Person (PEP) is defined as an individual who holds or has held one of the following offices or positions in or on behalf of Canada or a foreign country:

A head of state or government
A member of the executive council of government or member of a legislature
A deputy minster (or equivalent)
An ambassador or an ambassador's attaché or counselor
A military general (or higher rank)
A president of a state owned company or bank
A head of a government agency
A judge, or
A leader or president of a political party in a legislature.

A PEP also includes the following immediate family members of the individual described above:

- Spouse or common law partner
- Mother or Father
- Child
- Brother, Sister, Half-brother or Half-sister, or
- Spouse's or common-law partner's mother or father

Altimum is aware of the special requirements regarding Politically Exposed Persons and will ask its clients whether they fall within that category and will take such additional measures as is necessary if they do. The question asked is:

Are you or a member of your immediate family (spouse or common law partner, mother or father, child, brother, sister, half-brother or half-sister, or spouse's or common-law partner's mother or father) a person who holds or has held one of the following offices or positions in or on behalf of either Canada or a foreign country: head of state or government; a member of the executive counsel of government or member of a legislature; a deputy minister (or equivalent); an ambassador or an ambassador's attache or counselor' a military general (or higher rank); a president of a state owned company or bank; a head of a government agency, a judge, a leader or president of a political party in a legislature, or the Head of an International Organization? (Collectively known as a Politically Exposed Person, or PEP.)

Once we have determined that a person is a PEP we must take reasonable measures to establish the source of funds used for the transaction and the transaction must be reviewed by the Compliance Department within 14 days of the transaction.

One might be a Politically Exposed Foreign Person (PEFP) or a Politically Exposed Domestic Person (PEDP).

Head of an International Organization

The Head of an International Organization is referred to as an HIO. As with a PEP, the Approved Person must determine the source of funds and the Compliance Department must review the transaction within 14 days.

Under the PCMLTFA, several legislative requirements apply to Altimum Approved Persons and non-licensed employees.

Since November 8, 2001, the new law required Altimum Mutuals Inc. to identify and report suspicious transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC is responsible for the collection, analysis and disclosure of information in order to assist in the detection, prevention and deterrence of money laundering in Canada and abroad.

On June 23, 2008 Bill C25 came into effect introducing significant regulatory revisions to Bill C22.

Account Opening

For the opening of all new client accounts, Altimum completes a KYC Form and initial Trade Order Form, which are signed and dated by the Chief Compliance Officer, the Approved Person and the client. The client who signs is usually the person who will be providing investment instructions on the account. The KYC Form contains the client's bank information, i.e. name and address of bank and types of accounts held by the client. An Account will not be opened with any of the above information missing.

Forms of Identification

The rule before June 23 2008 was that client identification must be verified within 30 days of account opening, but that rule no longer applies. Client identification must now be obtained and verified prior to executing the first trade in the account.

Valid government-issued photo identification must be documented. You must record the document or record number of the photo identification together with the expiry date of the document onto the KYC Form. You may not use a provincial health card from Ontario since this is not an acceptable form of identification. (This is also true of Prince Edward Island and Manitoba health cards.) Cards which have expired must not be used for identification purposes.

If ID is outstanding, the Approved Person will not be paid for the account from the time of opening and no cheques will be issued to clients. No transactions can be placed and no additional funds can be deposited to the account until the requirements are met. If the requirements are still outstanding at the end of 90 days, the accounts will be closed, and the cost of any steps that must be taken to close the account will be charged back to the advisor, including commission reversals and market losses.

When you refer to a document to identify an individual, you have to be looking at an original. You cannot use a copy of the document to identify an individual. In cases where it is not possible for you to view the original yourself, you may choose an agent (i.e. notary public) to verify the original identification document on your behalf. Even if you use an agent, you are responsible for making sure that the identification requirements are met. If you have doubts about the information collected concerning an individual's previous identification, you must identify that individual again. If a client presents a tampered source of identification, do not proceed with the KYC form or with opening the account. Contact the Chief Compliance Officer immediately.

Type 1 Documentation	Type 2 Documentation
Driver's Licence issued in Canada	Provincial Health Card (without photo ID and/or expiry date) NOTE: Health Cards are not acceptable identification for Manitoba, Ontario or Prince Edward Island.
Passport	Birth Certificate — issued in Canada only (by the government; Church issue not accepted)
Certificate of Indian Status — issued by the Government of Canada	Social Insurance Card — issued by the Government of Canada (must be viewed by Advisor)
Canadian Permanent Residence Card	Major Credit Card (bearing the name of the individual and their signature)
Quebec Health Card (with photo ID and expiry date) NOTE: Health Cards in Quebec must be offered by clients — they cannot be requested.	College/University Student ID card (bearing the name of the individual, signature and photograph)
Identification Card — issued by Province (not available in Quebec)	Firearms Licence (Possession and Acquisition Licence) — issued federally by RCMP with photo ID
	NEXUS Card (bearing the name of the individual, passport number and photograph)
	CNIB Card
	Canadian Forces Identification Card (bearing the name of the individual, photograph and expiry date)
	Certificate of Canadian Citizenship or Naturalization

The Approved Person has to take reasonable measures to keep client information up to date. For high risk clients, such as clients who do not reside in Canada or for Politically Exposed Persons, reasonable measures include asking the client to confirm or update identification information every two years. In the case of corporations, or other entities, reasonable measures include consulting a paper or electronic record, or obtaining information verbally to keep client identification information up to date.

In order to comply with The Proceeds of Crime (Money Laundering and Terrorist Financing Act, PCMLTFA) and Bill C-25 every new Altimum account must include:

1. Valid identification such as a birth certificate, a driver's license or passport. The expiry date must also be noted if the document has one.
2. Employer information
3. Banking information
4. Foreign or domestic political involvement
5. Foreign or domestic positions of influence.

Altimum will establish the identity of the client or the individual with trading authorization on the account by reference to the individual's birth certificate, driver's licence, passport or other similar document. (A Provincial Health Card may not be used for identification in Ontario.) The Regulations require Altimum's Approved Persons to view an original birth certificate, driver's license or passport for the account holder. Approved Persons must meet face to face with clients in order to complete the account application. Approved Persons can not accept clients over the telephone. On Altimum's KYC Form, the Approved Person must enter the type of identification of the client that was viewed, and record the identification number and the expiry date of the document. Altimum will not open an account if proper identification is not provided.

Cash Transactions at Altimum Mutuals Inc.

Altimum will not accept cash from its clients for the purchase of mutual fund investments. Altimum in fact prohibits its Approved Persons from accepting cash from clients. Therefore no such transactions should be accepted or executed by any Approved Person. All purchase orders must be accompanied by a personal cheque or Pre-Authorized Debit form issued from a financial institution. A cheque must have the client's address pre-printed on the cheque. Many fund companies will not accept a cheque where the client has filled in the address themselves, nor will many accept a money order made out to the mutual fund company as the source of funds is not clear.

Altimum has each new client sign a form for this purpose, which forms part of the KYC form and will record the relevant office or position, the country, the source of funds that are being deposit into the account, and the date of the PEP determination on the form as required. The Approved Person is required to obtain prior authorization for each transaction from the Chief Compliance Officer. Accounts will not be opened if the form is not completed.

Obligation to Report

Altimum is aware that if it receives cash in the amount of $10,000 or more, it is required to keep and retain a Large Cash Transaction Record that indicates:

a. The name of the individual from whom the cash is received,
b. The individual's address, country of residence, and the nature of his or her principal business or occupation,
c. The date and the nature of the transaction,
d. The number of the client account that is affected by the transaction,
e. The amount and currency of the cash received.

As a mutual fund dealer, Altimum is required to report all attempted or completed suspicious transactions, terrorist property, and large cash transactions to FINTRAC, pursuant to the PCMLTRA. As such, all Altimum Approved Persons and non-licensed employees must immediately report such activities, in writing, to Altimum's Chief Compliance Officer, even if they were only attempted and never completed.

Suspicious Transactions

Suspicious transactions are financial transactions that elicit reasonable grounds to suspect the inclusion of monies related to the commission of a money laundering offence or terrorist activity financing offence. Approved Persons must report any transactions for which they have "reasonable grounds" to suspect that money laundering offence may have been committed and must also report any suspicious transactions attempted even if the transaction was not completed.

An assessment of a suspicious transaction should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's financial circumstances, financial history and trading patterns. The following are examples of common indicators that may point to a suspicious transaction:

- Client admits or makes statements about involvement in criminal activities;
- Client shows uncommon curiosity about internal systems, controls and policies;
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account;
- Client uses a variety of similar but different addresses;
- Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious;
- You are aware that a client is the subject of a money laundering or terrorist financing investigation;
- Client attempts to convince Approved Person not to compete any documentation required for the transaction;
- Client makes enquiries that would indicate a desire to avoid reporting;

- Client seems very conversant with money laundering or terrorist activity financing issues;
- Client produces seemingly false identification or identification that appears to have been counterfeited, altered or may be inaccurate;
- Client only submits copies of personal identification documents;
- Client wants to establish identity using something other than his or her personal identification documents;
- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past;
- Client makes cash transactions of consistently rounded-off large amounts (e.g. $9900, $8500, etc.);
- Client attempts to purchase investments with cash, money orders, traveller's cheques, cashier's cheques or other bank instruments, especially that are just under the reporting threshold amount of $10,000 in an apparent attempt to avoid the reporting threshold;
- The transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities;
- The transaction involves a 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;
- Client attempts to open or is operating accounts under a false name;
- Client opens an account with a large number of small cash deposits, then executes a small number of large cash withdrawals.
- A new or prospective client's background is not easily verifiable or reputation is questionable.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account.
- Client deals with or represents a third party when the identity of the beneficiary or counter party is undisclosed.
- Payment is made by way of third party cheques payable to, or endorsed over to, the client.
- Client requests transfers of funds and/or securities between accounts not known to be related.

Altimum together with the Chief Compliance Officer would be alert for suspicious activities with respect to the provision of cash to and the payment of cash by Altimum, such as repeated transactions just below the reporting requirements. Altimum is aware that persons who have received cash or other property from criminal activities often wish to conceal the source by converting the cash or property into other property such as securities.

Altimum together with the Chief Compliance Officer is also aware that a Dealer that receives cash for securities, knowing that the cash was, in whole or in part, obtained or derived directly or indirectly as a result of certain crimes, would commit the offence of laundering the proceeds of crime. (Criminal Code, Section 462.31) Upon noting any

suspicious activities, Altimum will report such activities to the proper law enforcement agencies.

Altimum will verify the identity of the individual who conducts the transaction without delay in a Large Cash Transaction Record:

1. Where the employee, director or Approved Person of Altimum who conducts the transaction on behalf of Altimum has reason to believe that the individual from whom the cash is received is acting on behalf of a third party,
2. Whether, according to that individual, the transaction is conducted on behalf of a third party and, if so, the information shown above for the third party, or that the individual himself purports to be keeping and retaining a Large Cash Transaction record in respect of receipt of the cash from the third party.
3. If the employee or director of Altimum who conducts any of the transactions on behalf of Altimum knows that two or more transactions are conducted by or on behalf of the same person on the same day and result in a total amount of cash being received of $10,000 or more, it will be treated as a single transaction, and will be subject to all above noted procedure (24-hour rule).

Altimum will establish the identity of the client or the individual with trading authorization on the account by reference to the individual's birth certificate, driver's licence, passport or other similar document. (A Provincial Health Card may not be used for identification in Ontario.) The type and reference number of such document will be indicated on the Large Cash Transaction Record. Proceeds of Crime (Money Laundering) Regulations, s. 11(2)(c) and (3).

In keeping with s. 19 of the Regulation, Altimum will keep the Large Cash Transaction Record in the client's file.

Record Keeping

Altimum relies on the records retained and maintained by its Approved Persons in order to fulfill its legislative requirements under the MCMLTFA, and when required, submits reports to FINTRAC which collects, analyzes and discloses financial information and intelligence on suspected money laundering and terrorist activities financing.

As such, it is essential that during the account-opening process, Approved Persons accurately update clients' records and retain the following pertinent documentation in the clients' files, including:

1. KYC Account applications signed by the individual authorized to give instructions and which sets out the bank account number in the name of the individual. A copy of a void cheque from the clients' bank account is sufficient to satisfy the bank account number requirement.

2. Every Trade Order Form, Account Application, trading authorization form, purchase/redemption/switch request form, and all correspondence that pertains to the operation of the account.
3. Guarantees,
4. Trade authorizations, (including Limited Trading Authorizations)
5. Powers of attorney,
6. Joint account agreements,
7. Identification
8. Copies of official corporate records (i.e. Articles of Incorporation)

Records must be kept for all large single cash transactions of $10,000 or more. Large cash transactions records are also needed when two or more cash transactions adding up to $10,000 are made by the same client within a 24-hour period.

Individuals with Trading Authorization

Identification must be documented for any client who has been assigned with trading authority on an account. You must verify identification of the authorized individuals on an account prior to executing the first trade on the account. Therefore, you must verify and document identification of clients who have been appointed with powers of attorney. (See the section in this manual for important restrictions regarding Powers of Attorney filed at Altimum). In the case of a business account, you do not have to identify any more than three individuals who are authorized to give instructions for the account. For greater clarification, that is to say that if there are two parties who can give instructions, you must identify both of them. If there are five, you need only identify the first three who present themselves (or at least three of the five.)

Sanctions will also be applied to accounts where identification is outstanding from individuals who have been granted trading authority on an account. These are identical to those identified in the previous section, Forms of Identification.

You do not have to identify any individuals authorized to give instructions on a registered Plan account such as an RRSP, a RRIF or a LIF.

Corporate Accounts and other entities

If you open an account for a corporation or other entity, in addition to the KYC form and account operating agreements, Approved Persons must retain copies of the official corporate records showing the provisions that relate to the power to bind the corporation regarding the account. This could be the Articles of Incorporation or Corporate Resolutions that set out those duly authorized to sign on behalf of the corporation, such as an officer, the comptroller, etc. If there were changes subsequent to the articles, then the board resolution stating the change is to be included in this type of record.

For greater clarity, you must confirm the existence of any corporation or other entity that opens an account. In the case of a corporation, in addition to confirming its existence, you must also determine the corporation's name, address and the names of each of its directors. The record you use to confirm a corporation's existence can be on paper or in an electronic version. It is not acceptable to verify the information verbally, such as over the telephone. You have to keep a copy of the record. You must obtain information about the corporation's beneficial ownership and document the corporate or tax identification number on the KYC form. You also have to submit the names of the corporation's directors and you must take identification from each of the directors, up to a maximum number of three. (See the section Individuals with Trading Authorization)

Third Party Determination

A third party is a person or corporation, that is not the account holder, but who has authority to give instructions regarding the account. The following conditions must be met for third party assignment on clients' accounts:

1 A copy of the trading authorization (i.e. Power of Attorney) is obtained. (See the section entitled Powers of Attorney in this manual.)
2 Government-issued identification must be verified and documented for all third parties. The procedure outlined in the preceding section "Ascertaining Identity" should be followed; and
3 The third party is not to be a resident of, and is not to be physically present in, a country that is a member of the Financial Action Task Force (FATF).

These countries can be identified at this website:
http://www1.oecd.org/fatf/Members_en.htm

Retention of Records

FINTRAC requires the retention of client records for a minimum of five years from the day they were created or the date of the last transaction conducted by the client. Additionally, MFDA Rule 5.6 requires that client records must be maintained for a minimum of seven years. Therefore, Altimum will retain all account opening and trade related records noted above for at least seven years following the closing of the account to which they relate. All other records will be retained for seven years following the day on which the records were created.

Failure to comply with record keeping requirements can lead to criminal charges against the Approved Person, launched by FINTRAC. Conviction of failure to retain records can lead to a maximum fine of $500,000, a maximum jail term of five years, or both (s.6).

Prohibited Disclosure to Clients

No person or entity shall disclose that they have made a report or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. Therefor an Approved Person is not to tell the client that a report has been filed under the Act.

Training of Staff and Compliance Regime

The Proceeds of Crime and Money Laundering Act requires dealers to implement a compliance regime that includes ongoing training, written policies and procedures, and risk assessment. A risk assessment has been completed by the Chief Executive Officer of Altimum.

Altimum has appointed the Chief Compliance Officer to be the Chief AML Officer with regard to monitoring Anti-Money Laundering and the Proceeds of Crime. The Chief Compliance Officer shall conduct audits to ensure that the procedures are being followed. Altimum together with the Chief Compliance Officer ensures that all staff is fully aware of the above policies and procedures on Money Laundering at all times. The Chief Compliance Officer ensures that staff is aware of this by providing staff with a copy of the written policies and procedures and testing their awareness with a written test. Participation in such training is mandatory for all Approved Persons and employees.

In the future, if registered staff will be dealing with client trade transactions, the Chief Compliance Officer will review daily transactions on a regular basis to ensure that staff I complying with the anti-money laundering policy. Any exceptions will be brought to the attention of staff by the Chief Compliance Officer and incorporated as part of the training program for staff. Testing for compliance with Anti-Money Laundering regulations will form part of sub-branch audits and will be conducted at least once every two years. The Compliance Officer will also ensure that he or she keeps up to date on all regulatory Anti-Money Laundering requirements.

All Approved Persons at Altimum must be aware of Policies and Procedures with relation to Money Laundering. An Approved Person who becomes suspicious of any account, transaction, or suspicious of a new or prospective client should report this information to the Head Office Chief Compliance Officer. Altimum will be responsible to report any suspicious transactions to FINTRAC within the required timeframe.

All aspects of the compliance program, including training, will be reviewed every two years to determine whether any corrections or updating is necessary.

Non-Compliance

New FINTRAC regulations include a series of penalties for non-compliance. They include the following:

1. Failure to report a suspicious transaction or failure to make a terrorist property report: up to five years imprisonment, $2 million fine or both.
2. Failure to report a large cash transaction or an electronic funds transfer: $500,000 fine for the first offence; $1 million fine for each subsequent offence.
3. Failure to retain records: up to 5 years" imprisonment, $500,000 fine or both
4. Failure to implement a compliance regime: up to five years' imprisonment, $500,000 fine or both.

Making Reports to FINTRAC

As a "reporting entity", we have a legal obligation to send a terrorist property report to FINTRAC if we have property in our possession or control that we know is owned or controlled by or on behalf of a terrorist group or listed person. This includes information about any transaction or attempted transaction relating to that property.

All Terrorist Group and Listed Person Property Reports must be sent by paper as they cannot be sent electronically.

There is no minimum threshold for reporting a transaction.

Electronic reporting

We must submit all reports electronically, if we have the technical capabilities to do so, except for the Terrorist Group or Listed Person Property Reports which can only be paper filed at this time.

Electronic reporting must be done by logging on to FINTRAC's secure web site (F2R). All reporting entities must register for and utilize F2R if they have the technical capability. Generally 'technical capability' means a computer and Internet access. This can be done via FINTRAC's website at www.fintrac.gc.ca.

Report acknowledgement and correction requests

FINTRAC will send us an acknowledgement message when our report has been received electronically. This will include the date and time our report was received and a FINTRAC-generated identification number. Keep this information for our records.

If our report contains incomplete information, FINTRAC may notify us. The notification will indicate the date and time our report was received, a FINTRAC-generated identification number, along with information on what must be completed.

Paper reporting

In the event we are unable to report electronically or we have to file a Terrorist Group and Listed Person Property Report, we must submit paper reports to FINTRAC. All Terrorist Group and Listed Person Property Reports must be sent by paper as they cannot be sent electronically.The following forms can be accessed and printed from FINTRAC's website or call 1-866-346-8722 for a copy to be faxed or mailed to us.

- Suspicious Transaction or Attempted Transaction Report (FINTRAC may refer to this report as a Suspicious Transaction Report)
- Large Cash Transaction Report
- Terrorist Group or Listed Person Property Report (FINTRAC may refer to this report as a Terrorist Property Report)

To ensure that the information provided is legible and to facilitate data entry, FINTRAC prefers the free-text areas of the paper report (such as, fields 1 and 2 of Part B) are keyed. If reports must be completed by hand, the use of black ink, and CAPITAL LETTERS is recommended.

There are two ways to send a paper report to FINTRAC:

1) Fax to 1-866-226-2346; or
2) Registered Mail to the following address:

Financial Transactions and Reports Analysis Centre of Canada,

Section A,
234 Laurier Avenue West, 24th Floor

Ottawa, ON

K1P 1H7

FINTRAC will not send us any acknowledgement when a paper report has been received.

Information to be contained in reports

The information to be contained in reports depends on the type of report being filed.

There are several parts that must be completed on both the Suspicious Transaction or Attempted Transaction Report form and the Large Cash Transaction Report form, but some parts are only to be completed if applicable. Any fields marked with an asterisk (*) must be completed.

All other fields require us to make a reasonable effort to get the information.

The information that is required to be provided includes:

- Information about the reporting entity (Altimum).
- Information about the transaction or attempted transaction and its disposition.
- Information about the individual conducting a transaction or attempting to conduct a transaction and/or the individual on whose behalf the transaction is being conducted or attempted to be conducted.
- Information explaining our reasons for suspicion and if we have taken action.

With Suspicious Transaction or Attempted Transaction Reports, we should record the details of the transaction or attempted transaction and why we felt it was suspicious.

Reporting under the Criminal Code of Canada

In addition to making a Terrorist Group or Listed Person Property Report to FINTRAC under the Act, the Criminal Code also has reporting requirements for terrorist property. These Criminal Code requirements apply to every person in Canada and any Canadian outside of Canada. It does not matter whether we are a reporting entity under the Act or not and we do not have to be involved in any life insurance transactions before we are subject to the Criminal Code requirements.

The Criminal Code requires us to disclose to the RCMP and CSIS the existence of property in our possession or control that we know is owned or controlled by or on behalf of a terrorist group or listed person. This includes information about any transaction or attempted transaction relating to that property. Information is to be provided to the RCMP and CSIS, immediately, at:

- RCMP - Financial Intelligence Task Force unclassified fax: (613) 993-9474.
- CSIS Financing Unit, unclassified fax: (613) 231-0266.

If we have property in our possession or control that we know or suspect is owned or controlled by or on behalf of a terrorist group or listed person, including information about any transaction or attempted transaction relating to that property, we may not complete or be involved in the transaction or attempted transaction. It is an offence under the Criminal Code to deal with any property if we know that it is owned or controlled by or on behalf of a terrorist group or listed person. It is also an offence to be involved in any transaction in respect of such property. In such circumstances, we are to remove ourselves from any involvement.

The Criminal Code has a 10-year maximum jail term for failure to report terrorist property to the RCMP and CSIS.

Reporting Requirements are found in the Act.

We are required to submit a Suspicious Transaction or Attempted Transaction Report (STATR) if we have reasonable grounds to suspect that a transaction or attempted transaction is related to a money laundering or terrorist activity financing offence. The reporting of suspicious activity will require us to exercise judgment.

As a "reporting entity", we also have a legal obligation to send a terrorist property report to FINTRAC if we have property in our possession or control that we know or suspect is owned or controlled by or on behalf of a terrorist group or listed person. This includes information about any transaction or attempted transaction relating to that property.

Required Written Records and Client Identification Obligations

Reporting entities are required to keep large cash transaction records if cash is accepted, which it is not at Altimum Mutuals Inc. Reporting entities are also required to maintain client information records. Other records that we are required to keep include records related to beneficial ownership, not-for-profit organizations, third party determinations, politically exposed persons and heads of international organizations.

Client information record

For an individual

We must ascertain and record the client's name, address, date of birth, the nature of the client's principal business or occupation, and the source of funds. If an individual is retired, we are required to record information about their principal business or occupation prior to retirement.

Client identity must be verified. This is true whether the transaction is conducted on the client's own behalf, or on behalf of a third party.
Unless otherwise specified, only original documents that are valid and have not expired may be referred to for the purpose of ascertaining identity. The identity is to be ascertained by reference to the individual's:

- Birth certificate;
- Driver's license;
- Passport; or
- Any similar record.

As we are required to ascertain the identity of an individual purchasing an investment fund, the client information record has to contain the individual's date of birth along with the type of identification document used to confirm the individual's identity, its reference number and its place of issue.

An Ontario Provincial Heath Card is not allowed to be used as identification.

For a corporation

We must ascertain the existence, name and address of the corporation, and the names of its directors. This can be done by reference to:

- Certificate of corporate status;
- A record that it is required to file annually under the applicable provincial securities legislation; or
- Any other record that ascertains its existence as a corporation.

Such a record may be in paper form or in an electronic version that is obtained from a source accessible to the public. If paper, the individual or entity ascertaining the corporate identity must retain the record or a copy of it. If electronic, a record must be kept setting out the corporation's registration number, the type of record referred to and the source of the electronic version of the record. If the corporation is a securities dealer, we do not have to ascertain the names of the corporation's directors.

For a non-corporate entity

We must confirm its existence by reference to a partnership agreement, articles of association, or any other similar record that confirms the entity's existence. We must keep a record of the type and source of records consulted or a paper copy of that record.

Beneficial owners record

If the client is a corporation, we must, at the time the existence of the corporation is confirmed, obtain,

- The name and, where required by a financial institution, occupation, of all directors of the corporation and, take reasonable measures to confirm and, keep a record of such.
- The name, address and, where required by a financial institution, occupation, of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation and,
- Information on the ownership, control, and structure of the corporation.

We must search through as many levels of information as necessary in order to determine beneficial ownership.

If there is no individual who owns or controls 25% or more of an entity we still keep a record of the measures we took and the information we obtained in order to reach that conclusion.

A beneficial owner cannot be another corporation or another entity.

For a Trust

If the client is a trust, we must obtain and keep a record of the names and addresses of all trustees and all known beneficiaries and settlors of the trust; and information on the ownership, control and structure of the trust.

Other Entities

If the client is an entity but not a corporation or a trust, we must, at the time the existence of the non-corporation entity is confirmed, obtain and keep a record of the name, address and, where required by a financial institution, occupation, of all persons who own or control, directly or indirectly, 25 per cent or more of the non-corporation entity; and information on the ownership, control, and structure of the entity.

If any of the information in this subsection cannot be obtained or its accuracy cannot be confirmed, we have to:

- Obtain the name of the most senior managing officer of the corporation, trust or other entity;
- Take reasonable measures to ascertain the identity of the most senior managing officer of the corporation, trust or other entity; and
- Treat that corporation, trust or other entity as high risk in our risk assessment document of our compliance regime.

We do not need to ascertain the identity of the most senior managing officer when there is no individual who owns or controls 25% or more of an entity.

In the context of this section, a senior managing officer of an entity may include but is not limited to its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any individual who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer. In the case of a sole proprietor or a partnership, the senior managing officer can be the owner or the partner.

We also have to keep a record of this information.

Keeping beneficial ownership information up to date is part of our ongoing monitoring obligations. The frequency with which we review beneficial ownership information and keep it up to date will vary depending on our risk assessment of our client. For high-risk clients, we will update beneficial ownership information more frequently and perform more frequent monitoring.

Ongoing Monitoring of Business Relationship and Related Records

Business relationship

A business relationship is a relationship that we establish with a client to conduct financial transactions or provide services related to those transactions. This term as it applies to anti money laundering and anti terrorist financing has been defined in order to clarify when a client is subject to enhanced monitoring.

We enter into a business relationship when we conduct two or more transactions in which we have to:

- Ascertain the identity of the individual or entity; or
- Confirm the existence of a corporation or other entity.

If we have a client who conducts two or more suspicious transactions, even if we are unable to ascertain the identity of the client, we have still entered into a business relationship with that client. This is because suspicious transactions require us to take reasonable measures to identify the client, and so two or more of these transactions will trigger a business relationship. We must treat this business relationship as high-risk, and undertake more frequent ongoing monitoring and updating of client identification information, as well as any other appropriate enhanced measures.

Once the business relationship is established, we must also:

- Conduct ongoing monitoring of our business relationship with the client; and
- Keep a record of the measures taken to monitor the business relationship and the information obtained as a result.

Ongoing monitoring

Ongoing monitoring means monitoring the business relationship with a client on a periodic basis. Using the risk assessment of the client with whom we have a business relationship we will determine how frequently we will monitor that business relationship. High-risk clients will be monitored more frequently and with more scrutiny than low-risk clients.

The risk assessment requires us to consider each one of the clients when assessing their risk for money-laundering and terrorist activities financing. However, an individual written assessment is not required for each client, so long as we can demonstrate that we put our client in the correct risk category, according to our policies and procedures and risk assessment. We have to perform ongoing monitoring of each business relationship to:

- Detect suspicious transactions that have to be reported;
- Keep client identification, beneficial ownership information, and the purpose and intended nature of the business relationship up to date;
- Reassess the level of risk associated with the client's transactions and
- Determine whether the transactions or activities are consistent with the information previously obtained about the client, including the risk assessment of the client.

Business Relationship Record

When we enter into a business relationship with a client, we have to keep a record of the purpose and intended nature of the business relationship.

We also have to review this information on a periodic basis and keep it up to date. This is done to ensure that we continue to understand clients' activities over time so that any changes can be measured to detect high risk, thus increasing the frequency of ongoing monitoring, updating of client identification information, and any other appropriate enhanced measures.

The frequency with which business relationship information is to be kept up to date will vary depending on our risk assessment of the client. We will monitor business relationships we consider high risk more frequently.

To obtain information on the purpose and intended nature of a business relationship, we can use the information we currently have about the client in our business records. If it's a new business relationship, one way of obtaining this information is to ask our client.

Not-for-profit organization record

If we have to confirm the existence of an entity that is a not-for-profit organization, we also have to do the following:

- Determine whether or not that entity is a registered charity for income tax purposes and keep a record to that effect. To make this determination, we can ask the client or consult the charities listing on the Canada Revenue Agency website (http://www.cra-arc.gc.ca).
- If that entity is not a registered charity, determine whether or not it solicits charitable financial donations from the public and keep a record to that effect. To make this determination, we can ask the client.

Third party determination record

A third party is an individual or entity other than the individual who conducts the transaction. When determining whether a "third party" is involved, it is not about who "owns" the money, but rather about who gives instructions to deal with the money. To determine who the third party is, the point to remember is whether the individual in front of us is acting on someone else's instructions. If so, that someone else is the third party.

If we are required to obtain a third party disclosure statement, that statement must include:

- The third party's name, address and principal business or occupation;
- Where the third party is an individual, date of birth;
- Where the third party is a corporation, the incorporation number and place of incorporation;
- Where the person or entity is acting on behalf of a third party, the nature of the relationship between the third party and the individual who signs the statement.
- Where the person or entity is not able to determine if the individual is acting on behalf of a third party but there are reasonable grounds to suspect that the individual is acting on behalf of a third party, a signed statement from the individual stating that they are not acting on behalf of a third party.

Record of Politically Exposed Person or Head of an International Organization

We must take reasonable measures to determine if a person is a politically exposed person or the head of an international organization, whether acting on their own behalf or on behalf of a third party and a record must be kept of that determination on the proper Altimum form, a sample of which can be found in this compliance manual immediately after the following revisions of June 2017.

It is important to note that for joint accounts each account holder must sign a separate form.

Canada

Politically exposed persons and heads of international organizations – Financial entities

June 2017

A politically exposed person (PEP) or the head of an international organization (HIO) is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO has puts them in a position to impact policy decisions, institutions and rules of procedure in the allocation of resources and finances, which can make them vulnerable to corruption.

Corruption is an international issue that impacts all countries, so the Financial Action Task Force (FATF) has recommended that all countries consider domestic as well as foreign politically exposed persons and heads of international organizations as part of the approach to combatting money laundering and the financing of terrorist activities. The FATF references the United Nations Convention against Corruption (UNCAC) which defines PEPs as "individuals who are, or have been, entrusted with prominent public functions and their family members and close associates".

Transparency International is an organization that operates internationally with a mandate to stop corruption and promote transparency. It can be a source of information to learn more about corruption and the potential vulnerability of persons who hold prominent positions.

Corruption can be defined simply as the misuse of public power for private benefit. Internationally, as well as within Canada's own anti-money laundering and anti-terrorist financing legislation, it is important to understand that the possibility for corruption exists, and that politically exposed persons or heads of international organizations can be vulnerable to carrying out, or being used for, money laundering or terrorist activity financing offences.

Part of knowing your clients is determining whether a person is a foreign PEP, a domestic PEP, a HIO, or a family member or close associate of one of these people.

The reporting entities with these obligations include financial entities, securities dealers, money services businesses and life insurance companies. This guidance is for financial entities who have to make a PEP or HIO determination in relation to account openings, the periodic review of existing accounts, the detection of a fact in relation to existing account holders, and incoming and outgoing electronic funds transfers (EFT) of $100,000 or more.

For all of these activities, you must take reasonable measures to determine whether a person is a foreign PEP, or a family member or close associate of a foreign PEP. Foreign PEPs, their family members and their close associates must automatically be treated as high-risk clients.

You must take reasonable measures to determine whether a person is a domestic PEP or HIO, or is a family member of a domestic PEP or HIO, at account opening, during the periodic review of existing account holders and for incoming and outgoing EFTs of $100,000 or more. You must also determine if there is a close association to a domestic PEP or HIO for incoming and outgoing EFTs of $100,000 or more, or if you detect a fact about an existing account holder.

Once you have determined that a person is a domestic PEP, a HIO, or the family member or close associate of a domestic PEP or HIO, you must assess to determine if that person poses a high risk for committing a money laundering or a terrorist activity financing offence. If you assess the risk to be high, then the person must be treated as a high-risk client.

All high-risk clients are subject to your policies and procedures for high-risk clients, outlined as a requirement of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). For high-risk PEPs, HIOs, their family members and close associates, you have specific obligations to keep records, establish source of funds, and obtain senior management review of a transaction, or approval to keep the account open.

If you have already determined that a person is a foreign PEP or the family member of a foreign PEP, in accordance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* (PCMLTFR), you are not required to make this determination again. Furthermore, you are not required to assess all of your existing account holders immediately upon the coming into force date (June 17, 2017) of the PEP and HIO obligations. Rather, FINTRAC expects you to have, within your policies and procedures, a process by which existing account holders will be assessed over time. This process should be in line with your obligation to take reasonable measures on a periodic basis to determine whether an account holder is a foreign PEP, a domestic PEP, a HIO, the family member of one of these people, or a close associate to a foreign PEP.

What reasonable measures should I use to make the determination?

You must take reasonable measures to determine whether a person is a PEP, a HIO, their family member or their close associate. You must also take reasonable measures if you are required to establish the source of funds for any account or EFTs of $100,000 or more for these persons.

Reasonable measures include, but are not limited to, one or more of the following actions:

1. asking the client;
2. conducting an open source search; or
3. consulting a source of commercially available information.

You may consider using more than one reasonable measure to make a determination.

How proactive or reactive your reasonable measures are is directly related to the specific obligation.

You must take reasonable measures to determine if a person is a **foreign PEP** or their **family member** or **close associate** at account opening, on a periodic basis for existing account holders, if a fact is detected about an existing account holder and for any EFT of $100,000 or more.

You must also take reasonable measures to determine if a person is a **domestic PEP**, a **HIO** or their **family member** at account opening, on a periodic basis for existing account holders and for any EFT of $100,000 or more. In addition to this, you must use reasonable measures to determine if a person is a **close associate** of a domestic PEP or HIO for any EFT of $100,000 or more, or if you detect a fact about an existing account holder.

In most cases a reasonable measures effort is proactive in that you must have a process in place to make the determination. For example, you may have a proactive process where, on a periodic basis, you run your list of account holders against an open source or a commercially available database. In this case, your reasonable measures parameters would need to be looking at whether an existing account holder is a foreign PEP, a domestic PEP, a HIO, the family member of any one of these or a close associate of a foreign PEP.

However, it is acceptable to have a reactive approach if you detect a fact outside of your normal periodic review that leads you to suspect a person is a PEP, a HIO, or their family member or close associate. You are not required to have policies and procedures in place to proactively seek out details about an existing account holder outside of your periodic basis. However, if a fact is detected, you must act on it. A detected fact could be one that constitutes reasonable grounds to suspect that an existing account holder is a **foreign PEP**, a **domestic PEP**, a **HIO**, or the **family member** or **close associate of any of these.**

For example, if your entity has media monitoring activities in place, and a fact is detected through these, it must be acted upon. There is no requirement, however, to have media monitoring activities in place for the purpose of detecting facts.

Who is a foreign PEP?

A **foreign PEP** is a person who holds or has held one 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 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; or
- leader or president of a political party represented in a legislature.

These persons are foreign PEPs regardless of citizenship, residence status or birth place.

A person determined to be a foreign PEP, is forever a foreign PEP.

Who is a domestic PEP?

A **domestic PEP** is a person who holds — or has held within the last 5 years — a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial government, or a Canadian municipal 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
- mayor*.

* In line with legislation across Canada, municipal governments include cities, towns, villages and rural (county) or metropolitan municipalities. As such, a mayor is the head of a city, town, village, or rural or metropolitan municipality, regardless of the size of the population.

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

Who is a head of an international organization?

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

1. the head of an international organization established by the governments of states; or
2. the head of an institution established by an international organization.

When we refer to the head of an international organization or the head of an institution established by an international organization we are referring to the primary person who leads that organization, for example a president or CEO.

There is no requirement for an institution established by an international organization to operate internationally. It is possible that an institution that has been established by an international organization only operates domestically, or in one jurisdiction.

You need to use reasonable measures to determine if the person is the head of an international organization or the head of an institution set up by an international organization.

Once a person is no longer the head of an international organization or the head of an institution established by an international organization, that person is no longer a HIO.

What is an international organization?

An international organization is an organization set up by the governments of more than one country. The key to determining whether you are dealing with a HIO is to determine how the organization was established. 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 a HIO. The existence of these organizations is recognized by law in their member countries but the organizations are not seen to be resident organizations of any one member country.

Certain organizations clearly meet this definition, but others may take more research before coming to a determination. Examples of international organizations, and institutions established by international organizations, can be found in Annex A of this guidance.

Why is it important to consider the family member or close associate of a PEP or HIO?

It is critical to consider family members or close associates of PEPs and HIOs as part of your PCMLTFA obligations. It is an established trend that criminals carrying out, or directing, criminal activity will distance themselves from the proceeds of that crime as much as possible until they have laundered the money. FINTRAC has observed that many criminals rely on family members or other personal relationships to conduct transactions on their behalf in order to create this distance until they can establish a safe way to spend these assets.

You may, therefore, not see joint accounts with, or financial transactions conducted between, a PEP or HIO and their family members or close associates. This is because the purpose of laundering funds is to protect the identity of the criminals and they may avoid a direct link with the individuals involved in conducting any transaction on their behalf. This is why FINTRAC's guidance references other types of associations to consider, beyond transactions or shared accounts, when making a close associate or family member determination.

Who is considered to be the family member of a PEP or a HIO?

If a person is a foreign PEP, domestic PEP or HIO, then certain family members must also be regarded as PEPs or HIOs. These **family members** are:

- their spouse or common-law partner;

- their child;
- their mother or father;
- the mother or father of their spouse or common-law partner; and
- a child of their mother or father (sibling).

Is the niece of a PEP considered a family member?

No. A person is a PEP or HIO because of the position that they hold or have held. The family members of the PEP or HIO that are specifically listed in this guideline are also regarded as PEPs or HIOs. If John is a PEP, then John's brother, Sam, is considered a PEP. But Sam's daughter (John's niece) is not determined to be a PEP under the PCMLTFA.

Is the step-child of a PEP or the step-child of a PEP's mother or father considered a family member?

A step-family relationship does not fall under the definition of a family member unless they were legally adopted. For example, if Helen is a domestic PEP, and she has legally adopted Sarah, her step-daughter through marriage, then Sarah is the child of a domestic PEP.

Similarly, if a marriage includes step-siblings the siblings are not considered family members if they were not legally adopted by the step-parent. For example, Angela marries a foreign PEP, and each has a daughter from a previous marriage. Neither Angela, nor the foreign PEP, adopts the other's daughter, so the two daughters are not considered as siblings to each other. Only Angela (legal spouse) and the foreign PEP's biological daughter need to be considered as family members of a foreign PEP.

Who is considered to be a close associate of a PEP or a HIO?

Certain activities or transactions will trigger your obligation to **take reasonable measures** to determine whether a person is a close associate of a foreign PEP, domestic PEP or HIO. A close associate can be an individual who is closely connected to a PEP or HIO for personal or business reasons. The term "close associate" is not intended to capture every person who has been associated with a PEP or HIO.

As a financial entity, you are required to take reasonable measures to determine if you are dealing with a **close associate of a foreign PEP**:

- at account opening;
- during your periodic review of existing account holders;
- when you send or receive an international EFT of $100,000 or more on behalf of a person;
- if you detect a fact, outside of your periodic review, about an existing account holder.

You are required to take reasonable measures to determine if you are dealing with a **close associate of a domestic PEP or HIO**:

- when you send or receive an EFT of $100,000 or more on behalf of a person;
- if you detect a fact, outside of your periodic review, about an existing account holder.

Your obligation to take reasonable measures to make a close associate determination exists regardless of whether the PEP or HIO also holds an account with you. For example, the PEP or HIO may hold an account at Bank ABC, while you hold the account of a person who is determined to be a close associate of the PEP or HIO.

A person determined to be a close associate of a foreign PEP must be treated as a high-risk client.

However, if you determine that a person is a close associate of a domestic PEP or HIO, you must conduct a risk assessment of that close associate. If you determine that the close associate is a high risk for a money laundering or terrorist activity financing offence, then you must treat that person as a high-risk client.

Some examples of a close association for personal or business reasons include a person who is:

- 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 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.

The examples provided are only a sample of considerations to assist you in identifying close associates. Because a close associate is not meant to be every person associated to a PEP or HIO, you will need to have a means to determine if this is a close association you need to identify and treat as such.

You need to use reasonable measures to determine if a person is a close associate to a PEP or HIO. However, financial entities that have actual knowledge of a close association must act on this, even if such association is not otherwise widely or publicly known.

The reasonable measures you take to identify a close association may include processes you already have in place for other purposes such as media monitoring; the ongoing monitoring of your business relationships; questions you ask of your clients; access to a database that outlines associations; or a third party credible source that identifies these connections between a PEP or HIO and your client.

When do I make the determination?

As a financial entity, there are four instances that will trigger your overall PEP and HIO obligations:

- account opening

- on a periodic basis for existing account holders
- if you detect a fact about an existing account holder
- when you conduct an EFT of $100,000 or more

Account-related determination

Account opening

When you open a new account for a person, you must take reasonable measures to determine if that person is a foreign PEP, a domestic PEP, a HIO, a family member of one of these people, or a close associate of a foreign PEP.

What do I do once the determination is made?

1. If you determine that the person is a **foreign PEP**, or a **family member** or **close associate of a foreign PEP**, you must take reasonable measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

   Within 30 days after the day the account is opened, you must take reasonable measures to determine whether the person is a foreign PEP, or a family member or close associate of a foreign PEP and establish the source of funds, as well as obtain the approval of a member of senior management to keep the account open.

2. If you determine that the person is a **domestic PEP**, a **HIO** or **a family member of a domestic PEP or HIO**, you must perform a risk assessment of that client to determine if the individual is a high risk for a money laundering or terrorist activity financing offence. If yes, you must take reasonable measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

   Within 30 days after the day the account was opened, you must take reasonable measures to determine whether the person is a domestic PEP, a HIO, or a family member of a domestic PEP or HIO, as well as conduct the risk assessment, and, if necessary based on the risk assessment, take reasonable measures to establish the source of funds and obtain senior management approval to keep the account open.

Existing account holders

On a periodic basis you must take reasonable measures to determine if an existing account holder is a foreign PEP, a domestic PEP, a HIO, a family member of one of these people, or a close associate of a foreign PEP.

What do I do once the determination is made?

1. If you determine that the person is a **foreign PEP**, or a **family member or close associate of a foreign PEP**, you must take reasonable measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

2. If you determine that the person is a **domestic PEP**, a **HIO** or a f**amily member of a domestic PEP or HIO**, you must perform a risk assessment of the person to determine if the individual is a high risk for a money laundering or terrorist activity financing offence. If yes, you must take reasonable measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

Detect a fact about an existing account holder

It is possible that outside of your periodic process, you detect a fact that that gives you reasonable grounds to suspect that an existing account holder is a foreign PEP, a domestic PEP, a HIO, or the family member or close associate of a foreign PEP, a domestic PEP or a HIO.

What does it mean to "detect a fact"?

The detection of a fact occurs outside of your periodic review of existing account holders. This obligation puts in place the requirement that you act on information you may happen across at any point during your relationship with an account holder. While there is no requirement to have proactive processes in place to detect facts about existing account holders, if you do have actual information related to a PEP or HIO determination obligation you must act on that information.

The information you may detect must be a fact that constitutes reasonable grounds to suspect that an account holder is a PEP, a HIO, or a family member or close associate of a PEP or HIO. Detecting this fact could occur through a disclosure made by an existing account holder, or activities such as media monitoring efforts you may already have in place, knowledge of domestic and world events, or a search that is run against an open source or third party database. When you become aware of a fact that constitutes reasonable grounds to suspect that an account holder is a PEP, a HIO, or a family member or close associate of a PEP or HIO, you must act on it.

While a name match is a fact, it is not necessarily a fact that constitutes reasonable grounds to suspect that your existing account holder is a PEP, a HIO or a family member or close associate of one of these. FINTRAC's expectation is that you would apply other parameters (e.g., address, date of birth, age, transaction activities, etc.) to the name match that would bring that name match to a point where it would constitute reasonable grounds to suspect that the existing account holder is a PEP or a HIO, or a family member or close associate of one of these.

Once you have detected a fact that constitutes reasonable grounds to suspect that a person is a **foreign PEP**, or **a family member or close associate of a foreign PEP**, you have 30 days to take reasonable measures to determine whether that person is actually such a person, and, if yes, obtain senior management approval to keep the account open and establish the source of funds in the account.

Once you have detected a fact that constitutes reasonable grounds to suspect that a person is a **domestic PEP**, or **HIO**, or a **family member or close associate of a domestic PEP or HIO**, you have 30 days to take reasonable measures to determine whether that person is actually such a person and, if yes, assess the risk of that person. If the risk assessed is high, you must also obtain senior management approval to keep the account open and take reasonable measures to establish the source of funds in the account within those 30 days.

Examples of how you may detect facts:

- A provincial election in Ontario leads to the election of Members of Provincial Parliament (MPPs). Because of the election, you run your list of client names against a credible third party database and determine that the full name of an account holder is the same as one of the newly elected MPPs. In addition, the date of birth on the account matches that of the elected MPP and the address on the account is within that MPP's riding. This is now a detected fact that constitutes reasonable grounds to suspect that an account holder is a domestic PEP. You must use reasonable measures to determine if that account holder is in fact the elected MPP or a family member or close associate of the MPP.
- The media monitoring activities you may have in place pick up the name of a newly appointed military general that is identical to the full name of an existing account holder. You then proceed to research the military general and discover that her base is located in the same city as the account holder. With this fact detected, you now have to take reasonable measures to determine if that existing account holder is in fact the military general, or a family member of, or closely associated to the military general.
- An existing account holder receives a series of wire transfers from a name that is recognized by one of your employees because of widespread media attention of an upcoming World Trade Organization (WTO) meeting and they recognize the name of the new director-general of the WTO who is a HIO. While this name match alone may not constitute reasonable grounds to suspect being a close associate of a HIO, certain parameters (e.g., where the transfers were generated, any applicable account information, the names of other entities involved in the transaction) may further strengthen the possibility that the wire transfer was sent by a HIO. Based on this detected fact, you must determine if your existing account holder may be closely associated to the director-general of the WTO.

What do I do once a fact is detected?

1. If you detect a fact that gives you reasonable grounds to suspect that an existing account holder is a **foreign PEP**, or a **family member or close associate of a foreign PEP**, you must take reasonable measures to determine if the account holder is in fact such a person. If you determine that the account holder is in fact such a person, you must take reasonable

measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

Within 30 days after the day on which you detect a fact that gives you reasonable grounds to suspect that the account holder is a foreign PEP, or their family member or close associate, you must determine whether the account holder is in fact such a person. If yes, then taking reasonable measures to establish the source of funds and obtaining senior management approval to keep the account open must also be completed within that same 30 days.

2. If you detect a fact that gives you reasonable grounds to suspect that an existing account holder is a **domestic PEP**, a **HIO**, their **family member or close associate**, you must take reasonable measures to determine if the account holder is in fact such a person. If you determine that the account holder is in fact such a person, you must perform a risk assessment of the person to determine if the individual is a high risk for a money laundering or terrorist activity financing offence. If yes, you must take reasonable measures to establish the source of the funds deposited or expected to be deposited into the account and obtain senior management approval to keep the account open. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

   Within 30 days after the day on which you detect a fact that gives you reasonable grounds to suspect that the account holder is a domestic PEP, a HIO, their family member or close associate, you must determine whether the account holder is in fact such a person. If yes, you must perform the risk assessment, and, if necessary based on the risk assessment, take reasonable measures to establish the source of funds and obtain senior management approval to keep the account open, all within that same 30 days.

Transaction-related determination

Incoming and Outgoing EFTs of $100,000 or more

When you send, at the request of a person, an EFT of $100,000 or more, or when you receive an EFT of $100,000 or more to be paid to a person who is the beneficiary, you must take reasonable measures to determine if the person who requests the EFT, or the beneficiary for whom you receive the EFT, respectively, is a foreign PEP, a domestic PEP, a HIO, or the family member or a close associate of a foreign PEP, a domestic PEP or a HIO.

If you are the intermediary to an EFT transaction, that is, a person requests that another entity initiate an EFT of $100,000 or more and that other entity uses you to carry out the transaction, you do not have the PEP determination obligations. Similarly, if an entity relays an EFT of $100,000 or more through you to another entity to be paid out to a beneficiary, you do not have the PEP determination obligations.

The PEP and HIO obligations rest with the entity asked to initiate an EFT of $100,000 or more or that will be paying the funds to the person who is the beneficiary of an EFT of $100,000 or more.

What do I do once the determination is made?

1. If you determine that the person who requests an EFT of $100,000 or more, or the person who is a beneficiary for whom you receive an EFT of $100,000 or more, is a **foreign PEP**, or a **family member or close associate of a foreign PEP**, you must have a member of senior management review the transaction. For outgoing EFTs, you must also take reasonable measures to establish the source of the funds for the transaction. As a high-risk client, the person must be subject to your policies and procedures for high-risk clients.

   Within 30 days after the day of the transaction, you must take reasonable measures to determine whether the person is a foreign PEP, or a family member or close associate of a foreign PEP, as well as have senior management review the transaction, and if necessary, establish the source of the funds for any outgoing EFT of $100,000 or more. You are not required to establish the source of funds for an incoming EFT of $100,000 or more.

2. If you determine that the person who requests an EFT of $100,000 or more, or the person who is a beneficiary for whom you receive an EFT of $100,000 or more, is a **domestic PEP**, a HIO, or a **family member or a close associate of a domestic PEP or HIO**, you must perform a risk assessment of the person or beneficiary to determine if the person or beneficiary is a high risk for a money laundering or terrorist activity financing offence. If yes, you must have a member of senior management review the transaction. For outgoing EFTs, you must also take reasonable measures to establish the source of the funds for the transaction.

   Within 30 days after the day of the transaction, you must take reasonable measures to determine whether the person is a domestic PEP, a HIO, or a family member or close associate of a domestic PEP or HIO, as well as conduct the risk assessment, and, if applicable, have senior management review the transaction, and establish the source of the funds for any outgoing EFT of $100,000 or more. You are not required to establish the source of funds for an incoming EFT of $100,000 or more.

Risk assessment of a PEP, HIO, family member, or close associate

If you determine that a person is a foreign PEP, or a family member of, or person closely associated with a foreign PEP, you must consider that person as high risk. As a high-risk client, you must proceed to establish the source of funds for the account or the transaction, and have a member of senior management review the transaction or approve keeping the account open.

If you determine that a person is a domestic PEP, a HIO, or a family member or close associate of a domestic PEP or HIO, your risk assessment must determine if this person is a high risk for a money laundering or a terrorist activity financing offence.

In all cases where you determine that a domestic PEP, a HIO, or a family member or close associate of a domestic PEP or HIO is a high-risk client, you must take reasonable measures to establish the source of the funds for the account or transactions, and have senior management review the transaction or approve keeping the account open.

You must consider that:

- foreign PEPs, and their family members and close associates are always high-risk clients;
- the risk assessment of domestic PEP and HIO clients, and their family members and close associates is needed as part of your risk-based approach;
- the measures you put in place in respect of each client are based on the level of risk assigned.

What could make a domestic PEP, a HIO, their family members or close associates high-risk?

To determine the level of risk for a domestic PEP or HIO, or the family member or close associate of a domestic PEP or HIO, you should consider the same indicators you already use to assess all of your clients. However, additional indicators may include:

- the amount of time that has passed since the person held the position – after 5 years a person is no longer considered a domestic PEP, so you may consider the length of time that has passed since the person held the position as an indication of risk;
- the organization or institution where the person held the position – there may be certain organizations that you determine are higher risk based on previously reported vulnerabilities to corruption;
- if the person attempts to shield their identity to prevent detection;
- the person makes use of intermediaries and this does not match the normal business practice;
- if the person makes use of family members or close associates as legal owners for property or corporate vehicles in a way that does not fit their expected profile;
- use of corporate vehicles (legal entities and legal arrangements) to obscure ownership;
- the person seems uncomfortable providing information about source of wealth or source of funds;
- the person is unable or reluctant to explain the reason for receiving or sending international EFTs of $100,000;
- Transparency International identifies certain industries as more vulnerable to corruption;
- the type of transaction(s) conducted or expected to be conducted by your client;
- a change in the account activity following their PEP, HIO, family member, or close associate status change;
- the person provides information you find to be inaccurate or incomplete;
- the person does not reveal additional positions they hold elsewhere;
- if the person owns or controls the financial institution or entity that is receiving the EFT of $100,000 or more.

Should you determine that a domestic PEP, a HIO, their family member or close associate is not a high risk, FINTRAC's expectation is that you will document this assessment as it supports how you will consider that client going forward, as per your compliance program's risk-based approach.

The documenting of an assessment can be done on a case-by-case basis or you could bucket or group your clients into categories of risk and treat these clients accordingly. In the course of a FINTRAC examination, you may be asked to demonstrate why a client meets the criteria of a particular risk category, so as to explain the way you are treating that client.

How do I establish the source of funds?

The requirement to establish the source of funds is linked to PEP and HIO clients that are determined to be high-risk. However, you may have a need to ask about the source of funds in the context of other obligations.

With respect to your high-risk PEP and HIO obligations, you must use reasonable measures to establish the source of funds used for the transaction, or that have been, will be, or are expected to be deposited into the account. For example, you could ask the client about the transaction or deposit or refer to source information available about the transaction or deposit. If your periodic review reveals account activity that is not in line with the information you have about the source of funds, one of the measures you may use is to follow up with your client to determine if there are reasons for this. If the information remains inconsistent with what you know about your client, or you are not satisfied with your client's response, and have reasonable grounds to suspect that the transaction is related to the commission or the attempted commission of a money laundering offence or of a terrorist activity financing offence, you must file a suspicious transaction report.

Who can review a transaction or allow an account to stay open?

A member of senior management can review a transaction and can allow an account to remain open. A member of senior management means an individual who has:

- authority to make and be held accountable for management decisions about transactions;
- awareness of the money laundering or terrorist financing risks to which financial entities are exposed; and
- awareness and understanding of the concepts of PEP, HIO, family member, and close associate.

If you are a sole proprietor with no employees, agents or other individuals authorized to act on your behalf, you are considered the senior manager.

Do I need to keep a record about the PEP, HIO, family member, or close associate?

Yes. You must keep a record after you determine that a person is a foreign PEP, a high-risk domestic PEP, a high-risk HIO, or a high-risk family member or high-risk close associate of one of these, AND senior management has reviewed the transaction, or you have obtained the approval to keep the account open. The information you have to record includes:

- 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, if known, that were used for the transaction or that are or are expected to be deposited in the account;
- the date you determined the individual to be a PEP, HIO, their family member or close associate;
- 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 or the account was approved.

You may also want to include in the record, the nature of the relationship between your client and the PEP or HIO, as applicable.

Retention: You must keep PEP and HIO account records for at least five years from the day the account to which they relate is closed.

Reasonable measures record

The regulations have been revised so that any time you are required to take reasonable measures you must keep a record if the reasonable measure is unsuccessful. A reasonable measure is unsuccessful when you do not obtain a response, such as a yes or no, so you are unable to make a conclusive determination. The record you need to keep for an unsuccessful reasonable measure must include:

- the measure taken;
- the date on which the measure was taken; and
- the reason why the measure was unsuccessful.

Because the reasonable measures your organization takes must be outlined in your policies and procedures, this can form part of your unsuccessful reasonable measures record, or you could document, on a case-by-case basis, the measure taken in each record for unsuccessful reasonable measures.

For example, you may document that you have an automated approach to run new or existing account holders against a commercial database that lists PEPs, HIOs, their family members and their associations. Similarly, your policies and procedures may indicate that you ask questions of your account holders on a periodic basis in order to keep this and other account information up to

date. Since the reasonable measures your entity takes are documented in your policies and procedures, this can form part of the record of unsuccessful reasonable measures. You then must document the reason why any reasonable measure was unsuccessful, and the date the reasonable measure was taken.

Should you take a measure that is not included in your policies and procedures, you would have to include details of that measure taken in your record of unsuccessful reasonable measures.

This obligation to document unsuccessful reasonable measures, however, applies to other obligations as well, such as establishing the source of funds.

Examples of documenting unsuccessful reasonable measures:

1. If, during your periodic review of clients to determine PEP or HIO status, you called more than once and left a message for your client and the client did not call back, then your record would need to indicate the measure you took, the date you did this and the fact that the client did not respond.
2. If you ask a high-risk domestic PEP, who is conducting an outgoing EFT, to tell you the source of the funds they are sending to outside of Canada and the person does not want to specify the source, your record must indicate that you asked your client for the source of funds information, the date you did this and that the person refused to provide the information.

You have 30 days from the account opening, the time of the transaction, or the detection of a fact, to take and document your reasonable measures.

There are two scenarios where you may want to consider an approach that allows you to clearly demonstrate that you are considering your clients appropriately and in line with your compliance program's risk-based approach.

1. The record-keeping obligations apply to unsuccessful reasonable measures. There is no requirement to keep a record if you determine that a person is a domestic PEP, HIO, their family member or, if applicable, close associate, and assess that person as low risk. However, during a FINTRAC examination, you may be asked to demonstrate that you conducted the risk assessment for a domestic PEP and HIO in accordance with your risk-based approach.
2. If you receive a negative response to a reasonable measure taken to determine if a person is a PEP or HIO, or their family member or close associate, recording this response would show that a determination was carried out. During a FINTRAC examination, FINTRAC may ask you to demonstrate how you applied your policies and procedures for PEP or HIO obligations.

Examples of records you may consider keeping:

1. If you asked your client at account opening if they were a domestic PEP or HIO, or family member of one, and your client responded "yes", but you assessed the client as a low risk, then your record could indicate that you asked the person, and that you assessed the person is a low risk.
2. If you conducted an open source internet search and did not find any information to suggest that your client is a PEP or HIO, or a family member of one of these, then you could record the

measure taken and that the results did not suggest a PEP or HIO status for the person.

Risk-based approach considerations

You are required to maintain up-to-date information about your existing account-based clients. This includes determining, on a periodic basis, if existing account holders are, or have become, PEPs, HIOs, family members of one of those persons, or persons who are closely associated with a foreign PEP.

Given that this determination must be made on a periodic basis, you may consider timing this obligation with your existing requirements to conduct ongoing monitoring of your business relationships for the purpose of updating client identification, beneficial ownership information and the purpose and intended nature of the business relationship.

To determine if existing account holders have become PEPs, HIOs, family members of one of those persons, or persons who are closely associated with a foreign PEP, you could ask your account-based clients to confirm the information you have on record. Alternatively, you may choose to run your list of clients against a credible open or third party information source, on a pre-determined schedule.

You are already required to assess any potential threats and vulnerabilities to money laundering and terrorist financing to which your business is exposed. As part of the overall assessment of client-risk you may want to consider offices or positions that are not prescribed to be those of a foreign or domestic PEP because you may deem these other offices or positions to also be vulnerable to being used for money laundering or the financing of terrorist activities.

You may also want to consider other international organizations, for example, organizations operating across multiple jurisdictions but not necessarily created by governments, if you think they could also be vulnerable to being used for money laundering or the financing of terrorist activities. Similarly, you are required to determine the head of an international organization, the primary person who leads that organization, but part of your risk assessment may indicate there are additional senior positions that you may want to consider because they also have the ability to make financial or contractual decisions for the entity.

As part of your risk assessment processes, you may determine that some individuals, not prescribed as family members, could be considered as a close associate of a PEP or HIO.

All of these considerations may impact the risk assessment of your client and serve to elevate the level of risk associated to that client.

What do you mean by enhanced ongoing monitoring?

Ongoing monitoring means that you have to monitor your client on a periodic basis. This requirement to conduct ongoing monitoring applies to more than just PEPs and HIOs and can consist of the same activities for PEPs and HIOs as it does for other clients. With a high-risk client,

you have to conduct enhanced ongoing monitoring, which is monitoring on a more frequent basis and incorporates different monitoring activities.

You could consider the following measures to monitor high-risk clients:

- reviewing transactions on a schedule to identify those that management must approve;
- preparing reports or performing more frequent reviews of reports that identify high-risk transactions;
- flagging unusual activities and elevating your concerns as necessary;
- setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

There are additional measures you can take to mitigate the risk of all high-risk clients, which can include:

- obtaining additional information on the client (e.g., occupation, assets, information available through public databases, Internet, etc.);
- obtaining information on the source of funds or source of wealth of the client;
- obtaining information on the reasons for intended or conducted transactions;
- obtaining the approval of senior management to enter into or maintain the business relationship;
- identifying patterns of transactions that need further examination;
- increased monitoring of transactions of higher-risk products, services and channels;
- establishing more stringent thresholds for ascertaining identification;
- gathering additional documents, data or information, or taking additional steps to verify the documents obtained;
- establishing transaction limits;
- increasing awareness of high-risk activities and transactions;
- increasing internal controls of high-risk business relationships;
- obtaining the approval of senior management at the transaction level for products and services that are new for that client.

Table 1 – Summary of PEP and HIO obligations

Triggering Activities	Determination	How a determination is made	Obligations	Record Keeping

Account opening Periodic monitoring of existing account holders Detect a fact for existing account holders EFTI or EFTO of $100,000 or more	Foreign PEP	Take reasonable measures for all of the triggering activities to determine if the person is a **foreign PEP** or a **family member** or **close associate** of a foreign PEP. If the determination is **yes**, you must carry out the associated obligations.	**Action to take if a determination is made:** Take reasonable measures to establish the source of the funds that have been, will be or are expected to be deposited into the account or that are used for an outgoing EFT. Ensure that a member of senior management reviews the transaction or approves keeping the account open. Apply policies and procedures for high-risk clients. Part of that includes enhanced ongoing monitoring of the account activities to detect suspicious transactions that must be reported.	**You must record:** • 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, if known, that were used for the transaction or that have been, will be or are expected to be deposited into the account; • the date you determined the individual to be a PEP, HIO, their family member or close associate; • the name of the member of senior management who reviewed the transaction or approved
	Domestic PEP or HIO	Take reasonable measures at account opening, or as part of your periodic review, to determine if a person is a **domestic PEP**, a **HIO**, or a **family member** of one of those persons. A determination is made because a fact is detected that identifies an existing account holder as a **domestic PEP**, a **HIO**, or their **family member** or **close associate**. Take reasonable measures to determine if the person sending or receiving an EFT of		

	$100,000 or more, is a **domestic PEP**, a **HIO**, or **their family member** or **close associate**. If the determination is yes, **AND** you assess the client as a high risk for a money laundering or terrorist financing offence, you must carry out the associated obligations.		keeping the account open; and, • the date the transaction was reviewed or the account was approved to stay open. You may want to include the nature of the relationship between your client and the PEP or HIO, as applicable.

Note: If you have made a successful determination for a PEP, HIO or their family member or close associate, you must complete the associated obligations within 30 days after the day of the account opening, detection of a fact, or the transaction, as applicable.

Note: A person determined to be a foreign PEP is forever a foreign PEP. A person ceases to be a domestic PEP 5 years after they have left the office. Once a person is no longer the head of an international organization, that person is no longer a HIO.

Annex A: Examples of international organizations and institutions established by international organizations

African Development Bank Group (http://www.afdb.org/en/) (Established by the Agreement Establishing the African Development Bank)

Arctic Council (http://www.arctic-council.org/index.php/en/document-archive/category/4-founding-documents) (Established by the Declaration on the Establishment of the Arctic Council)

Asian Development Bank (https://www.adb.org/about/main) (Established by the Agreement Establishing the Asian Development Bank – ADB Charter)

Association of Southeast Asian Nations (ASEAN) (http://asean.org/) (Established by the Asean Declaration)

Bank for International Settlements (https://www.bis.org/) (Established by the Constituent Charter of the Bank for International Settlements)

Basel Committee on Banking Supervision (https://www.bis.org/bcbs/) (Established by the Basel Committee on Banking Supervision Charter)

Caribbean Development Bank (http://www.caribank.org/) (Established by the Agreement Establishing the Caribbean Development Bank)

Commonwealth (http://thecommonwealth.org/) (Established by the Balfour Declaration, Statute of Westminster and London Declaration)

Community of Democracies (https://www.community-democracies.org/) (Warsaw Declaration)

Council of Europe (http://www.coe.int/en/) (Established by the European Convention on Human Rights)

European Bank for Reconstruction and Development (http://www.ebrd.com/home) (Established by the Agreement Establishing the European Bank for Reconstruction and Development)

European Free Trade Association Secretariat (http://www.efta.int/) (Established by the European Free Trade Agreement Convention)

European Space Agency (http://www.esa.int/ESA) (Established by the Convention for the establishment of a European Space Agency)

Inter-American Development Bank (IDB) (http://www.iadb.org/en/inter-american-development-bank,2837.html) (Established by the Agreement Establishing the Inter-American Development Bank)

International Criminal Court (https://www.icc-cpi.int/) (Established by the Rome Statute of the International Criminal Court)

International Commission of Missing Persons (http://www.icmp.int/) (Established by the Agreement on the status and functions of the International Commission on Missing Persons)

International Criminal Police Organization (http://www.interpol.int/) (Established by the Constitution of the ICPO-INTERPOL)

International Energy Agency (https://www.iea.org/) (Established by the Agreement on an International Energy Program)

International Energy Forum (https://www.ief.org/) (Established by the International Energy Forum Charter)

International Joint Commission (http://www.ijc.org/en_/) (Established by the Boundary Waters Treaty)

International Mobile Satellite Organization (http://www.imso.org/public/Home) (Established by the Convention on the International Maritime Satellite Organization)

International Organization for Migration (http://www.iom.int/) (Established by the Constitution of the Intergovernmental Committee for European Migration)

International Seabed Authority (https://www.isa.org.jm/) (Established by the United Nations Convention on the Law of the Sea)

International Telecommunications Satellite Organization (http://www.itso.int/index.php?option=com_content&view=article&id=46&Itemid=55&lang=en) (Established by the Agreement relating to the International Telecommunications Satellite Organization)

International Union for Conservation of Nature (https://www.iucn.org/) (Established by the formal act of 1948 constituting the International Union for Protection of Nature)

La Francophonie (http://www.francophonie.org/Welcome-to-the-International.html) (Established by the l'Agence de Coopération Culturelle et Technique (ACCT) Convention)

North Atlantic Treaty Organization (NATO) (http://www.nato.int/) (Established by the North Atlantic Treaty)

Organization for Economic Co-operation and Development (https://www.oecd.org/) (Established by the Organisation for Economic Co-operation and Development Convention)

Organization for Security and Co-operation in Europe (http://www.osce.org/) (Established by the Helsinki Final Act)

Organization of American States (http://www.oas.org/en/default.asp) (Established by the Charter of the Organization of American States)

Permanent Court of Arbitration (https://pca-cpa.org/en/home/) (Established under Article 20 of the 1899 Hague Convention for the Pacific Settlement of International Disputes)

World Customs Organization (http://www.wcoomd.org/en.aspx) (Established by the Convention establishing a Customs Co-operation Council)

Examples of institutions established by international organizations

United Nations (http://www.un.org/en/sections/about-un/overview/index.html) (Established by the Charter of the United Nations)

- Food and Agriculture Organization of the United Nations (http://www.fao.org/home/en/) (Established by the Constitution of the Food and Agriculture Organization)
- International Civil Aviation Organization (http://www.icao.int/Pages/default.aspx) (Established by the Convention on International Civil Aviation)
- International Labour Organization (http://www.ilo.org/global/lang--en/index.htm) (Established by International Labour Organization Constitution)
- International Maritime Organization (http://www.imo.org/en/Pages/Default.aspx) (Established by the Convention on the International Maritime Organization)
- International Monetary Fund (http://www.imf.org/external/index.htm) (Established by the Articles of Agreement of the International Monetary Fund)

- International Telecommunication Union (http://www.itu.int/en/Pages/default.aspx) (Established by the International Telegraph Convention. However, in 1934 the International Telegraph Convention of 1865 was then combined with the International Radiotelegraph Convention of 1906 to form the International Telecommunication Convention.)
- United Nations Educational, Scientific and Cultural Organization (UNESCO) (http://en.unesco.org/) (Established by the Constitution of UNESCO)
- World Bank Group (http://www.worldbank.org/) (Established by the Bretton Woods agreements)
- World Health Organization (http://www.who.int/en/) (Established by the constitution of the World Health Organization)
- World Intellectual Property Organization (http://www.wipo.int/portal/en/index.html) (Established by the Convention Establishing the World Intellectual Property Organization)
- World Meteorological Organization (http://public.wmo.int/en) (Established by the World Meteorological Convention)
- World Tourism Organization (http://www2.unwto.org/) (Established by the Statutes of the World Tourism Organization)
- Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization (https://www.ctbto.org/) (Established by the Comprehensive Nuclear-Test-Ban Treaty)
- International Atomic Energy Agency (https://www.iaea.org/) (Established by the Statute of the International Atomic Energy Agency)
- Organisation for the Prohibition of Chemical Weapons (https://www.opcw.org/) (Established by the Chemical Weapons Convention)
- World Trade Organization (https://www.wto.org/) (Established by the Marrakesh Agreement)

The Association of Southeast Asian Nations (ASEAN) established the:

- Economic Research Institute for ASEAN and East Asia (ERIA) (http://www.eria.org/) established by the adoption of the formal statement agreed to at the 3rd East Asia Summit in Singapore

The North Atlantic Treaty Organization (NATO) established the:

- NATO Communication and Information Agency (NCI Agency) (http://www.nato.int/cps/en/natohq/topics_69332.htm) established by the NCIO Charter, which transferred and amalgamated the functions of various agencies into the NCI Agency
- NATO Support and Procurement Organization (NSPO) (http://www.nspa.nato.int/en/index.htm) established by the NSPO Charter, which merged the names and roles of two NATO agencies into NSPO

Date Modified:

2018-07-11

ALTIMUM RESIDENCY AND CITIZENSHIP DECLARATION FOR NON-REGISTERED ACCOUNTS

Definitions:

PEP	**Politically Exposed Person**
PEFP	**Politically Exposed Foreign Person**
PEDF	**Politically Exposed Domestic Person**
HIO	**Head of an International Organization**
TIN	**Tax Identification Number, the equivalent of a SIN (or SSN in the U.S.)**

PART 1

1. **Are you a resident of a country outside of Canada or the United States?**

   If yes, specify country _____

   TIN number _____

2. **Are you a U.S. citizen or a U.S. connected person?**

   _____Yes _____No

   If so, you are because: (Check all that apply.)

   _____U. S. Citizenship

   _____Place of Residence in the U.S.

   _____U. S. birthplace

   _____I am a child of a U. S. citizen, my parents(s) is/are U. S. citizens.

   If you have answered yes, please provide your Social Security Number or Individual Taxpayer Identification Number here:

   SSN/TIN number _____

3. **Are you:**

   _____ A citizen of Canada _____ A landed Immigrant _____ Neither one

4. **Please answer the following question: (For Joint Accounts, each account holder must sign a separate form).**

   Are you or a member of your immediate family (spouse or common law partner, mother or father, child, brother, sister, half-brother or half-sister, or spouse's or common-law partner's mother or father) a person who holds or has held one of the following offices or positions in or on behalf of either Canada or a foreign country: head of state or government; a member of the executive counsel of government or member of a legislature; a deputy minister (or equivalent); an ambassador or an ambassador's attache or counselor' a military general (or higher rank); a president of a state owned company or bank; a head of a government agency, a judge, a leader or president of a political party in a legislature, or the Head of an International Organizaiton? (Collectively known as a Politically Exposed Person, or PEP.)

   _____Yes _____No

5. **Client address_____City_____Province ____ Postal Code_____**

PART 2 (ADVISOR NOTE; If the answer in Part 1 above is 'Yes' the client must complete Part 2.)

A. **Is the client personally a PEFP? PEDF? HIO? _____ Yes _____ No If so,which? _____ Proceed to Question C.**

B. **Is a family member of the client a PEP? _____Yes _____No If yes, state the family relationship _____**

C. **What is the relevant Office or Position? _____**

D. **What country? _____**

E. **What is the source of funds for deposit to this account? _____**

Please submit all relevant documentation to Altimum Mutuals Inc. Compliance

FOR JOINT ACCOUNTS EACH PERSON MUST SIGN A SEPARATE DECLARATION

BY SIGNING BELOW I DECLARE THAT THE ABOVE IS TRUE AND ACKNOWLEDGE THAT I HAVE RECEIVED A COPY OF THIS FORM.

Client Signature _____ Client Name_____ Date _____

Rep Signature _____Rep Code 7767 _____ Date of Determination _____

Compliance Officer Approval (Signature) _____ Date _____

Altimum Mutuals Inc.

Anti-Money Laundering Quiz

1. More stringent policies regarding the PCMLTFA come into effect

a) June 17, 2008
b) June 23, 2008
c) June 28, 2008

2. Which entity is responsible for collecting, analyzing and disclosing financial information and intelligence on suspected money laundering and terrorist activities financing?

a) FINTRAC
b) FINSCO
c) LIMRA

3. Money laundering involves criminal activity to:

a) Lend money from a financial institution to a foreign country
b) Moving money from one client's account to another client.
c) Transform dirty money into clean money.

4. Which of the following is false?

a) Money laundering may extend to property derived from illegal activities from any part of the world
b) When confirming the identification of a client, you must review the original document and not a photocopy
c) Terrorist financing never involves funds raised from legitimate sources.

5. Large cash transactions refer to a cash (or cash equivalent) value of:

a) $ 10,000
b) $ 100,000
c) $ 3,000

6. Valid photo-identification must be reviewed and documented for:

a) Clients or individuals with trading authorization on their accounts.
b) Individuals who attempt to trade but are prevented before becoming clients.
c) Both a) and b).

7. FINTRAC requires the retention of clients' records for a minimum of:

a) 5 years
b) 7 years
c) 10 years

8. All staff and Approved Persons must report suspicious transactions to Altimum's Compliance Department within:

a) 2 days
b) Immediately
c) 24 hours

9. Which of the following is not required to be reported to the Compliance Department?

a) When viewing the evening news, you discover that your client is the subject of a terrorist financing investigation.
b) Your client provides you with two cheques, each in the amount of $9,600 and asks that they are deposited on two different days during a one-week period.
c) Your client's relative passes away and he/she inherited $10,400. which is submitted for investing.

10. Which of the following is true regarding terrorist property? It…

a) Includes property of known terrorists that are listed on FINTRAC's website.
b) Is defined as the property that is seized by FINTRAC and the PCMLTFA.
c) May include property that is controlled by a client on behalf of a terrorist group.

11. Suspicious transactions are financial transactions that may include:

a) Transactions under the reporting limits.
b) Transactions requested by a client who produces seemingly counterfeited identification.
c) Both a) and b)

12. When opening a corporate account, which of the following must be obtained?

a) Letters Patent.
b) Articles of Incorporation.
c) Corporate Bylaws to determine signing authority.

13. When ascertaining identity, photo-identification must be verified, except for:

a) Individuals with trading authorization on non-registered accounts
b) Planholders of non-registered accounts
c) Individuals giving instructions on RRSPs accounts using Powers of Attorney

14. Which of the following is not an acceptable means of verifying a client's identification?

a) Relying on a notarized copy of an acceptable identification.
b) Accepting a copy of a current identification that was faxed directly from the client's office
c) Viewing the client's original identification and his/her home and documenting the information accordingly.

15. When opening a corporate account, the advisor must ascertain the identity of:

a) Less than three individuals who are authorized to give instructions on the account.
b) Up to three individuals who are authorized to give instructions on the account.
c) As many individuals as are authorized to give instructions on the account.

16. In circumstances where a client wishes to invest money that you know, rather than suspect, is related to property owned by a terrorist group, you should:

a) Proceed with the transaction, but report it to the Compliance Department.
b) Proceed with the transaction, as you are not responsible for its ties to terrorist financing.
c) Report this matter to the Compliance Department.

17. "Cash transactions" excludes:

a) Bank notes
b) Coins
c) Certified cheques

18. Terrorist property may include property in one's possession that is controlled on behalf of a terrorist, such as:

a) Cash, mutual fund shares, but not real estate.
b) real estate and common stock but not mutual funds invested in an RRSP.
c) Mutual funds held in RRIF's, LIF's, RRSP's, but not RESP's.

19. Failure to comply with record keeping requirements can lead to criminal charges with the following maximum penalties:

a) Up to 5 years' imprisonment and a fine of $500,000.
b) A fine of $50,000.
c) Up to 5 years' imprisonment and a fine of $2,000,000.

20. Which of the following is true?

a) FINTRAC requires advisors to retain a photocopy of their clients' identification.
b) FINTRAC requires the review of original, valid photo identification, and the recording of the registration number and expiration date of the document
c) FINTRAC requires advisors to review original, valid photo identification and to record the registration number of the document.

21. What is a PEP?

a) A Personal Exception Principle
b) A Politically Exposed Person
c) A Private Equity Purchase
d) A Physical Entity Provision

22. When identifying an individual, you may not use which two methods together:

a) a credit check (with their permission) and a cheque that has cleared their bank.
b) a sample void cheque showing their account information and a driver's licence from which you will record the number and the expiry date.
c) a call to the bank to verify that they have an account, and an attestation concerning an identification document for the individual from a commissioner of oaths.

23. When identifying an individual, you may use which two methods in combination:

a) a driver's licence from which you will record the number and the expiry date together with a reference to their credit file (with their permission)
b) a cleared cheque together with a verbal confirmation from the bank of a deposit account.
c) a driver's licence from which you will record the number and the expiry date together with a cleared cheque or a verbal confirmation from the bank of a deposit account.

24. All of the following are new requirements except for which one?

a) You must record the principal business or occupation of the individual.
b) You must record the intended use of the funds.
c) You must record the individual's date of birth.

25. Which statement is not correct?

a) You must identify any individual or entity who opens an account for a corporation.
b) You must identify any individual or entity who opens an account for a not-for-profit organization.
c) You must identify any individual giving instructions on someone else's account.
d) You need only identify individuals if they are opening an account in their own name for $10,000 or more.

26. Which of these four elements is not a correct requirement when establishing a AML compliance regime?

a) The appointment of a Supervisor of Anti-Money Laundering Procedures.
b) The development and application of policies and procedures to ensure compliance.
c) Periodic review of the effectiveness of policies and procedures.
d) Implementation of an ongoing compliance training program.

Name_____Rep Code_____Date_____

Mark_____ Pass/Fail_____

Compliance Officer Signature _____

Anti-Money Laundering and Risk Assessment

Financial Institution Name	**Altimum Mutuals Inc.**
Address of Principal Location	**94 Barbican Trail St. Catharines, ON L2T 4A8**
Name and Title of individual completing this questionaire	**Edith G. Reid Chief AML Officer**
Date this questionnaire was completed	**16-May-08**
Name of principal regulator	**Mutual Fund Dealers Association (MFDA)**

Has your institution appointed a senior officer responsible for its Anti-Money Laundering and Anti-Terrorist Financing program?	Yes	
Do the responses below apply to your institution's domestic branches in the country of head office jurisdiction	Yes	
Do the responses below apply to your institution's foreign subsidiaries and branches		N/A
General AML Policies, Practices and Procedures:		
Does the AML compliance program require approval of the Financial Institution's Board or a senior committee thereof	Yes	
Does the FI have a legal and regulatory compliance program that includes a designated compliance officer that is responsible for coordinating and overseeing the AML program on a day-to-day basis, which has been approved by senior management of the FI?	Yes	
Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions that has been approved by senior management?	Yes	
In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	Yes	
Does the FI have a policy prohibiting accounts/relationships with shell banks?		N/A
Does the FI have policies covering relationships with politically exposed persons consistent with industry best practices?	Yes	
Does the FI have appropriate record retention procedures pursuant to applicable law?	Yes	

Does the FI require that its AML policies and practices be applied to all branches and subsidiaries of the FI both in the home country and in locations outside of the home country?	Yes	
Risk Assessment		
Does the FI have a risk focused assessment of its customer base and transactions of its customers?	Yes	
Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	Yes	
Know Your Client, Due Diligence, and Enhanced Due Diligence		
Has the FI implemented systems for the identification of its clients including client information in the case of recorded transactions, account opening, etc?	Yes	
Does the FI have a requirement to collect information regarding its customers' business activities?	Yes	
Does the FI collect information and assess its FI customers' AML policies or practices?		N/A
Does the FI have procedures to establish a record for each customer noting their respective identification documents and KYC information collected at acocunt opening?	Yes	
Does the FI take steps to understand the normal and expected transactions of its clients based on its risk assessment of its clients?	Yes	
Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds		
Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	Yes	
Does the FI have procedures to identify transactions structured to avoid large cash reporting requirements?	Yes	
Does the FI screen transactions for customers or transactions the FI deems to be of significantly high risk that special attention to such clients or transactions is necessary prior to completing any such transactions?	Yes	

Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products?	Yes	
Does the FI have policies to reasonably ensure that tit only operates with correspondent banks that possess licenses to operate in their countries of origin?		N/A
Transaction Monitoring		
Does the FI have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments?	Yes	
AML Training		
Does the FI provide AML training to relevant employees that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	Yes	
Does the FI retain records of its training sessions including attendance records and relevant training materials used?	Yes	
Does the FI have policies to communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	Yes	
Does the FI employ agents to carry out some of the functions of the FI and if so does the FI provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	Yes	

Risk Assessment

Altimum Mutuals Inc.

Products, Services, Delivery Channels and Geographic Locations

	Yes	No	N/A
Identify whether you provide any of the following products, services or delivery channels.			
Do you offer services that make it difficult to fully identify clients?		**No**	
Do you offer electronic funds payment services?		**No**	
Do you offer any of the following: **Electronic cash (for example stored value and payroll cards)?** **Funds transfers (domestic and international)?** **Automated banking machines (ABMs)?**		**No**	
Do you offer any of the following: **International correspondent banking services involving transactions such as commercial payments for non-clients (for example, acting as an intermediary bank) and use of carriers or couriers for international transport of cash, monetary instruments or other documents (pouch activities)?** **Services involving banknote and precious metal trading and delivery?** **Electronic banking?** **Private banking (domestic and international)?** **Foreign correspondent accounts?** **Trade finance activities (letters of credit)?** **Lending activities, particularly loans secured by cash collateral and marketable securities?** **Non-deposit account services (for example, non-deposit investment products and insurance)?** **Accounts through which you can extend cheque or bank draft writing privileges to the clients of other institutions, often foreign banks (pass through or payable through type accounts)?** **Services involving an immigrant investor program?** **Non face-to-face transactions, such as Internet services, by mail or by telephone?**		**No**	
Identify whether you deal with clients or provide products or services in the following geographic locations:			
Is the client located in a known high crime rate area?		**No**	
Do you or your clients operate or undertake activities in the following countries: **Any country subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN)? In some circumstances, this will include sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized.** **Any country identified as a financial secrecy haven or jurisdiction?** **Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement? You can consult the current**		**No**	

non-cooperative countries and territories listed on the FATF Web site at http://www.fatf-gafi.org (select the "Current NCCT list" tab).
Any country identified by credible sources:

- **as lacking appropriatemoney laundering or terrorist financing laws and regulations?**
- **as providing funding or support for terrorist activities?**
- **as having significant levels of corruption, or other criminal activity? Credible sources means information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly available. Such sources may include, but are not limited to, international bodies such as the World Bank, the International Monetary Fund, the Organisation for Economic Co-operation and Development, and Transparency International as well as relevant national government bodies and non-governmental organisations.**

Identify whether any of the following apply to the client:

Is the client a cash intensive business?	**No**
Does the client's business generate large amounts of cash for certain transactions that are not normally cash intensive?	**No**
Is the client an intermediary or "gatekeeper" such as a professional that holds accounts for clients where the identity of the underlying client is not disclosed to you?	**No**
Does the client use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering or anti-terrorist financing obligations?	**No**
Does client identification take place other than face-to-face?	**No**
Does the client reside outside Canada?	**Occ**
Does the client deal offshore?	**No**
Is the client an unregistered charity or other unregulated "not for profit" organisation (especially one operating on a "cross-border" basis)?	**No**

Identify whether any of the following apply to the client:

Is the client located in a known high crime rate area?	**No**
Has the client been identified to have engaged in activity that is consistent with the indicators for your sector identified in Guideline 2: Suspicious Transactions?	**No**
Does the comparison between your clients with similar profiles and high levels of assets or large transactions seem unreasonable?	**No**
Does the knowledge of local laws, regulations and rules seem excessive for your client?	**No**
Is the client a new client?	
Do your clients use intermediate vehicles (such as corporations, trusts, foundations, partnerships) or other structures that do not seem usual for their business or seem very complex and unnecessary?	**No**
Does the client offer on-line gaming?	**No**
Does the client's structure or nature of its business or relationship make it difficult to identify the true owners or controllers?	**No**
Is there a significant and unexplained geographic distance between you and the location of the client?	**No**
Is there frequent and unexplained movement of accounts or funds between institutions in various geographic locations or to different institutions?	**No**

Identify whether any of the following apply to the client:

Is the client a politically exposed foreign person?	**No**

A politically exposed person is an individual who holds or has ever held one of the following offices or positions in or on behalf of Canada or a foreign country:

- **a head of state or government;**
- **a member of the executive council of government or member of a legislature;**
- **a deputy minister (or equivalent);**
- **an ambassador or an ambassador's attaché or counsellor;**
- **a military general (or higher rank);**
- **a president of a state-owned company or bank;**
- **a head of a government agency;**
- **a judge; or**
- **a leader or president of a political party in a legislature.**

A politically exposed person also includes the following family members of the individual described above:

- **mother or father;**
- **child;**
- **spouse or common-law partner;**
- **spouse's or common-law partner's mother or father and**
- **brother, sister, half-brother or half-sister (that is, any other child of the individual's mother or father).**

For financial entities: **N/A**

- **Is the client a foreign financial institution with which you have a correspondent banking relationship?**
- **Is the client a correspondent bank that has been subject to sanctions?**

Risk Level Assessment Matrix

Altimum Mutuals Inc. has determined its level of risk to be LOW.

Low

Stable, known client base
No electronic transaction services or the website is informational or non-transactional
There are few or no large currency transactions.
Identified a few high-risk clients and businesses
Few international accounts or very low volume of currency activity in the accounts
A limited number of fund transfers for clients, non clients, limited third-party transactions, and no foreign funds transfers
Your business is located in an area known to have low crime rate.
No transactions with high-risk geographic locations
Low turnover of key anti-money laundering personnel and frontline personnel (i.e., client service representatives, tellers, or other personnel)

Moderate

Client base increasing due to branching, merger, or acquisition
You are beginning electronic transaction services and offer limited products and services.
There is a moderate volume of large currency or structured transactions.
Identified a moderate number of high-risk clients and businesses
Moderate level of international accounts with unexplained currency activity
A moderate number of fund transfers, a few international fund transfers from personal or business accounts with typically low-risk countries
Your business is located in an area known to have moderate crime rate.

Minimal transactions with high-risk geographic locations
Low turnover of key anti-money laundering personnel, but frontline personnel may have changed

High

A large and growing client base in diverse geographic area
You offer a wide array of electronic transaction services (i.e., account transfers, or accounts opened via the Internet).
There is a significant volume of large currency or structured transactions.
Identified a large number of high-risk clients and businesses
Large number of international accounts with unexplained currency activity
Frequent funds from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions
Your business is located in an area known to have high crime rate.
Significant volume of transactions with high-risk geographic locations
High turnover, especially in key anti-money laundering personnel positions

Reviews and amendments to the Proceeds of Crime Compliance Program

This program was adopted on

Document Revision History

Date	What changed?	Reason for the change

Self-review

To test effectiveness, a review of compliance policies and procedures, assessment of business' risks related to money laundering and terrorist financing including risk mitigation measures, and training is conducted every two years.

These reviews will help determine if my/our business has policies and procedures in place to comply with legislative and regulatory requirements, and whether those policies and procedures are being adhered to.

Date of review: _____

Name of person completing review: _____

Signature of principal/advisor: _____

Compliance items	Yes	No	Comments, Testing/Evidence of effectiveness
Appointment of a compliance officer			
1. I/We have appointed a Compliance Officer for the practice.			
Written compliance policies and procedures			
2. Within the past two years, I/we have reviewed the criteria and process for identifying and reporting suspicious transactions and terrorist property and have established policies and procedures in this regard.			
3. I/We are aware of and abide by the requirements under the legislation for record keeping.			
4. I/We have reviewed the requirements under the legislation for client identification and verification and collect all information required on product applications, or as required, for each particular line of business.			
5. I/We have reviewed the legislated requirements with respect to reporting large cash transactions and where applicable comply with the requirements.			
Money laundering and terrorist financing risk evaluation			
6. Within the past two years, I/we have reviewed and documented my/our business' exposure to risk and have taken special measures to lower high risks.			
Ongoing compliance training			
7. I/We have established standards for the frequency and method of training with documentation on file.			

8. Details of the specific training material (i.e., what training was completed, who completed the training and when was it completed) are documented and on file? If not, provide details here.			
Actions required:			
Details of follow-ups completed:			

CSA/ACVM Canadian Securities Administrators | Autorites canadfennes en valeurs mobilieres

CSA Guide to Monthly Suppression of Terrorism and Canadian Sanctions Reporting

("STCS Guide"}

Introduction

Registrants, exempt dealers, and exempt advisers **(firms)** can refer to this guide when preparing monthly reports under suppression of terrorism and Canadian sanctions laws.

The guide is intended to assist firms and is not a substitute for legal advice.

Federal Provisions

Canada's laws against terrorist financing and sanctioned individuals and entities are contained in federal Canadian statutes and regulations, such as the *Criminal Code* (Canada).

The *Criminal Code* (Canada) and any current or future laws relating to the suppression of terrorism or Canadian sanctions are referred to in this guide as **Federal Provisions.**

Monthly STCS Reports

Under some Federal Provisions, firms are required to determine whether they have the property of Designated Persons.[1]

In some cases, those Federal Provisions will also require firms to file a monthly report **(Monthly STCS Reports)** to their provincial securities regulator **(Principal Regulator).**

This includes the reporting of a *Nil* response even when the firm determines that it does not possess or control a Designated Person's property.

Currently, firms are only required to file Monthly STCS reports under the *Criminal Code* (Canada) and the *Justice for Victims of Corrupt Foreign Officials Act.*

Firms can use the following lists as a guide when filing Monthly STCS Reports:

- https://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-284/FullText.html

[1] Each Federal Provision includes a list of Designated Persons. Not all Federal Provisions use the same defined term when referring to such persons or entities. Examples of the defined terms used in various Federal Provisions include: "designated person" "listed entity", "listed person", "person associated with Al-Qaida", "person associated with the Taliban", and "foreign national". These terms are often used interchangeably when discussing sanctions, although regulations are specific in their usage of the terms.

- https://laws-lois.justice.gc.ca/eng/regulations/SOR-2017-233/page-2.html#h-842596

Reports are submitted on the 14th day of each month, to the Principal Regulator. A senior officer of the firm, preferably the Chief Compliance Officer, should sign the monthly report.

Overview of certain duties

In addition to the Monthly STCS Report requirement, there are other obligations included in Federal Provisions, outlined at a high level below.

We remind firms that provincial securities regulators only receive the Monthly STCS Reports.

Canadian federal entities are responsible for the Federal Provisions. Firms should contact these federal entities or their legal counsel with any questions regarding their obligations.

Duty to determine: Designated Persons

Firms are required to determine whether they have the property of a Designated Person. This could include property owned or controlled by the Designated Person.

When firms are reviewing their process to determine a Designated Person, the Government of Canada's Economic Sanction Page may be helpful: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng.

The Listed Person subsection may be particularly relevant:
https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/listed_persons-personnes_inscrites.aspx?lang=eng

In some cases, consolidated lists have been created.

- the Consolidated Canadian Autonomous Sanctions List includes the names of any listed persons (both individuals and entities) in the schedules of regulations made under the *Special Economic Measures Act* and the *Justice for Victims of Corrupt Foreign Officials Act*: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng

- regulations made under Canada's *United Nations Act* refer to Designated Persons as listed by the relevant United Nation's Security Council Committee. The Consolidated United Nations Security Council Sanctions List is also available on the United Nations web site: https://www.un.org/securitycouncil/

In other cases, stand alone lists are provided, such as for the *Justice for Victims of Corrupt Foreign Officials Regulations* and *Criminal Code*:

- https://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-284/FullText.html
- https://laws-lois.justice.gc.ca/eng/regulations/SOR-2017-233/page-2.html#h-842596

Freezing property

Federal Provisions usually do not allow any person in Canada and any Canadian outside Canada to knowingly:

- deal, directly or indirectly, with property of a Designated Person,
- enter into or facilitate, directly or indirectly, any transaction in respect of such property, or
- provide any financial or other services for or for the benefit of a Designated Person.

Please refer to the text of a specific Federal Provision for clarity on prohibited dealings and activities.

Duty to disclose – RCMP and CSIS

Federal Provisions usually require any person in Canada and any Canadian outside Canada to immediately report any property or transactional information related to a Designated Person, to either the Royal Canadian Mounted Police (**RCMP**) or the Canadian Security Intelligence Service (**CSIS**) or both (depending on the Federal Provision).

Information can be provided to these organizations as follows:

RCMP

Anti-terrorist Financing Team

Unclassified fax: 613-825-7030

CSIS

Financing Unit

Unclassified fax: 613-369-2303

There are also additional reporting requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which require the submission of a terrorist property report to the Financial Transactions and Reports Analysis Centre of Canada (**FINTRAC**).

For instructions relating to the preparation and submission of this report, reporting entities should visit the FINTRAC website at: **http://www.fintrac-canafe.gc.ca.**

Conclusion

Please note that there are other Federal Provisions for which the Government of Canada does not provide up to date lists. Firms will need to have procedures in place to ensure they are monitoring for all applicable Designated Persons.

Federal Provisions are updated frequently. It is important that firms review their procedures and this guide periodically. CSA staff recommend that this be done monthly.

Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

Terrorist Property Report

Use this form if you are a reporting person or entity and you have property in your possession or control that you know is owned or controlled by or on behalf of a terrorist or a terrorist group or you believe that the property is owned or controlled by or on behalf of a listed person.

A terrorist or a terrorist group includes anyone that has as one of their purposes or activities facilitating or carrying out any terrorist activity. A listed person means anyone listed in the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. A terrorist group or a listed person can be an individual, a corporation, a group, a trust, a partnership or a fund. It can also be an unincorporated association or organization.

For more information about who is considered a reporting person or entity and for instructions on how to complete this form, refer to FINTRAC's reporting guidance for your sector at: http://www.fintrac-canafe.gc.ca or call FINTRAC's toll-free enquiries line at 1-866-346-8722. **This report CANNOT presently be submitted electronically.**

Send completed form by mail: FINTRAC, Section A, 234 Laurier Avenue West, 24th Floor, Ottawa, Ontario K1P 1H7
or send completed form by fax: 1-866-226-2346

Is this Report a correction to a Report previously submitted?

☐ **NO**

REPORTING DATE 2 0 ____ ____ ____ (YEAR / MONTH / DAY)

TIME ____ ____ (HOUR / MINUTE)

☐ **YES**

- Enter the original Report's Date and Time

  Date 2 0 ____ ____ ____ (YEAR / MONTH / DAY) Time ____ ____ (HOUR / MINUTE)
- COMPLETE PART A – whether the information has changed or not
- Provide the new information ONLY for the affected fields in Part B through Part H
- If removing information from a field, strike a line through the field

All fields of the report marked with an asterisk (*) must be completed. The ones that are also marked "where applicable" must be completed if they are applicable to you or the property or transaction being reported. For all other fields, you have to make reasonable efforts to get the information.

PART A — Information about the person or entity filing this report

1. Reporting person or entity's identifier number* (where applicable)

2. Reporting person or entity's full name*

3. Street address*

4. City*

5. Province* 6. Postal code*

Whom can FINTRAC contact about this report?

7. Contact – Surname* 8. Contact – Given name* 9. Contact – Initial/Other

10. Contact – Telephone number (with area code)* 10A. Contact – Telephone extension number

11. Which of following types of reporting persons or entities best describes you?*

- ☐ **A** Accountant
- ☐ **B** Bank
- ☐ **C** Caisse populaire
- ☐ **D** Crown agent (sells/redeems money orders)
- ☐ **E** Casino
- ☐ **F** Co-op credit society
- ☐ **G** Credit union
- ☐ **H** Life insurance broker or agent
- ☐ **I** Life insurance company
- ☐ **J** Money services business
- ☐ **K** Provincial savings office
- ☐ **L** Real estate broker or sales representative
- ☐ **M** Securities dealer
- ☐ **N** Trust and loan company
- ☐ **O** Dealer in precious metals and stones (effective December 30, 2008)
- ☐ **P** Public notary and notary corporation of British Columbia (effective December 30, 2008)
- ☐ **Q** Real estate developer (effective February 20, 2009)

→

Canada

NOTE: Please copy this page for each additional, related, suspicious transaction (if required).

PART B — Reason for filing this report

Transaction ☐ of ☐

1. Please describe clearly and completely what led you to file this report about terrorist property.* Provide as many details as possible to explain how you came to be in possession or control of the property. If there is not enough room on the form, attach a separate sheet to provide all the relevant information. Make sure to indicate that this information belongs in field 1 of Part B.

2. Provide as many details as possible about how you know this property is owned or controlled by or on behalf of a terrorist or a terrorist group or about how you believe that this property is owned or controlled by or on behalf of a listed person.

Also include details of what other action you have taken regarding the property, in addition to sending this report to FINTRAC.
If there is not enough room on the form, attach a separate sheet to provide all the relevant information. Make sure to indicate that this information belongs in field 2 of Part B.

Note: You must disclose this property's existence to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service, along with any information about a transaction or proposed transaction for that property. For more information refer to FINTRAC's reporting guidance for your sector.

Information about the terrorist, terrorist group or listed entity

Name of terrorist group, listed person or individual that owns or controls the property (or that the property is owned or controlled on behalf of). If it is an entity, complete field 3. If it is an individual, complete fields 3A-B-C.

3. Full name of terrorist group or listed person

3A. Surname of terrorist or listed person

3B. Given name of terrorist or listed person

3C. Other/Initial

4. Street address

5. City

6. Province or state

7. Country

8. Postal or Zip code

9. Phone number (with area code)

9A. Phone extension number

Information about anyone who owns or controls the property on behalf of the terrorist or listed person above (where applicable)

Name of entity or individual that owns or controls the property on behalf of the terrorist or listed person named in field 3 or fields 3A-B-C (above). If it is an entity, complete field 10. If it is an individual, complete fields 10A-B-C

10. Full name of terrorist group or listed person

10A. Surname of individual

10B. Given name

10C. Other/Initial

11. Street address

12. City

13. Province or state

14. Country

15. Postal or Zip code

16. Phone number (with area code)

16A. Phone extension number

NOTE: Please copy this page for each additional property (if applicable).

Property ☐ of ☐

PART C — Information about the property

1. Type of property*

A ☐ **Cash**	Indicate the type of currency in property identifier (field 2) below. Indicate the actual or approximate value of the cash in field 4 below and provide the currency code applicable in field 4A. Provide any additional information about the cash in the description of property (field 5) below.
B ☐ **Bank account**	Indicate the name of the financial institution in property identifier (field 2) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide the account number(s) and other account information in Part D. If you need to provide any additional information about the account, you can use the description of property (field 5) below.
C ☐ **Insurance policy**	Indicate the name of the insurance policy issuer in property identifier (field 2) below, and policy number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 below and provide the currency code applicable in field 4A. Provide any additional information about the insurance policy in the description of property (field 5) below, such as the names of beneficiaries, etc.
D ☐ **Money order**	Indicate the name of issuer in property identifier (field 2) below, and any number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the money order in the description of property (field 5) below, such as the name of the bearer, etc.
E ☐ **Real estate**	Indicate the type of real estate (such as single family home, condo, commercial, land only, etc.) in property identifier (field 2) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the real estate in the description of property (field 5) below, such as the municipal address and name of registered owner, and description of the property.
F ☐ **Securities**	Indicate the name of the securities issuer in property identifier (field 2) below, and any securities number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the type of securities (such as stocks, bonds, mutual funds, etc.) in the description of property (field 5) below. If the property involves an account, complete Part D to provide information about the account.
G ☐ **Traveller's cheques**	Indicate name of issuer of the traveller's cheques in property identifier (field 2) below, and any number(s) in property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the traveller's cheques in the description of property (field 5) below, such as the currency, name of the bearer, etc.
H ☐ **Other**	DESCRIPTION (OTHER) For example, this could include the commercial assets of a business or partnership. Indicate property identifier (field 2) below, and property identifier number (field 3) below. Indicate the actual or approximate value in field 4 (below) and provide the currency code applicable in field 4A. Provide any additional information about the property in the description of property (field 5) below. If the property involves an account, complete Part D to provide information about the account.

2. Property identifier (see instructions above for type of property)

If there is not enough room to provide all the property identifier information for this property, attach a separate sheet to provide all the relevant information. Make sure to indicate that this information belongs in field 2 of Part C.

3. Property identifier number (see instructions above for type of property)

If there is not enough room to provide all the property identifier numbers for this property, attach a separate sheet to provide them all. Make sure to indicate that this information belongs in field 3 of Part C.

4. Property value (actual or approximate)*

4A. Currency code

Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, refer to FINTRAC's guidance for submitting reports by fax or mail.

5. Description of property

If there is not enough room to provide all the information to describe this property, attach a separate sheet to provide all the details. Make sure to indicate that this information belongs in field 5 of Part C.

NOTE: Please copy this page for each additional account (if applicable).

PART D — Account information (if property involves an account)

Property ☐ Account ☐ of ☐

1. Branch or transit number* (where applicable)

2. Account number* (where applicable)

3. Type of account* (where applicable)

A ☐ Personal B ☐ Business C ☐ Trust D ☐ Other DESCRIPTION (OTHER)

4. Currency code* (where applicable) Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, refer to FINTRAC's guidance for submitting reports by fax or mail.

5. Full name of each account holder* (where applicable)

A

B

C

6. Date opened YEAR MONTH DAY

7. Date closed 2 0 YEAR MONTH DAY

8. Status of the account* (if there was a transaction or a proposed transaction, please provide the status at the time the transaction was initiated or proposed.)

A ☐ Active B ☐ Inactive C ☐ Dormant

NOTE: Please copy this page for each additional, related transaction or proposed transaction (if required).

PART E1 — Information about any transaction or proposed transaction (where applicable)

Property ☐ Transaction ☐ of ☐

If there was a transaction related to the property, indicate how it was initiated, i.e., where the money came from. If there was a proposed transaction related to the property, indicate how it was proposed to be initiated.
If there was no transaction related to the property, do not complete this Part, or Parts E2, F, G or H.

1. Date of transaction* (where applicable)
2 0 ____ ____ ____
YEAR MONTH DAY

2. Time of transaction
____ ____
HOUR MINUTE

4. Date of posting (if different from date of transaction)
2 0 ____ ____ ____
YEAR MONTH DAY

or

3. Night deposit indicator* (where applicable)
☐

5. Type of funds or other property involved in initiating the transaction* (where applicable)

- A ☐ Cash
- B ☐ Diamonds
- C ☐ Incoming electronic funds transfer
- D ☐ Jewellery
- E ☐ Negotiated bank draft
- F ☐ Negotiated cheque
- G ☐ Negotiated life insurance policy
- H ☐ Negotiated money order
- I ☐ Negotiated securities
- J ☐ Negotiated traveller's cheques
- K ☐ Precious metals
- L ☐ Precious stones (excluding diamonds)
- M ☐ Real estate
- N ☐ Redeemed casino chips
- O ☐ Withdrawal from account
- P ☐ Other ____ DESCRIPTION (OTHER)

6. Amount of transaction* (where applicable)
____

7. Currency code* (where applicable) Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, refer to FINTRAC's guidance for submitting reports by fax or mail.
____

Additional information about the funds described in field 5 above

8. Other institution, entity or person name and number* (where applicable)
____

9. Other institution, entity or person account number* (where applicable)
____

10. How was the transaction conducted?* (where applicable)

- A ☐ In-branch/Office/Store
- B ☐ Automated banking machine
- C ☐ Armoured car
- D ☐ Courier
- E ☐ Mail deposit
- F ☐ Phone
- G ☐ Other ____ DESCRIPTION (OTHER)

11. ID number of the individual initially identifying a transaction for property described in Part C
____

NOTE: Please copy this page for each additional, related, disposition (per transaction) (if required).

PART E2 — Information about the transaction or proposed transaction disposition(s) (where applicable)

Property ☐ Transaction ☐ Disposition ☐ of ☐

If there was a transaction related to the property, indicate how it was completed, i.e., where the money went. If there was a proposed transaction related to the property, indicate how it was proposed to be completed. If there was no transaction related to the property, do not complete this Part, or Parts E1, F, G or H.

Indicate on whose behalf this transaction was conducted.

On behalf of:

- ☐ **The individual who conducted the transaction** (described in PART F)
- ☐ **An entity (other than an individual)** (also complete PART G)
- ☐ **Another individual (besides the individual who conducted it)** (also complete PART H)

12. Disposition of funds how the transaction was completed* (where applicable)

- A ☐ Cash out
- B ☐ Currency exchange
- C ☐ Deposit to an account
- D ☐ Life insurance policy purchase/deposit
  - POLICY NUMBER
- E ☐ Outgoing electronic funds transfer
- F ☐ Purchase of bank draft
- G ☐ Purchase of casino chips
- H ☐ Purchase of diamonds
- I ☐ Purchase of jewellery
- J ☐ Purchase of precious metals
- K ☐ Purchase of precious stones (excluding diamonds)
- L ☐ Purchase of money order
- M ☐ Purchase of traveller's cheques
- N ☐ Real estate purchase/deposit
- O ☐ Securities purchase/deposit
- P ☐ Other
  - DESCRIPTION (OTHER)

13. Amount of disposition* (where applicable)

14. Currency code* (where applicable) Enter CAD if Canadian dollars or USD for United States dollars. If another type of currency is involved, refer to FINTRAC's guidance for submitting reports by fax or mail.

Additional information about the funds described in field 12 above

15. Other institution, entity or person name and number* (where applicable)

16. Account number or policy number of other institution, entity or person* (where applicable)

NOTE: Please copy this page for each additional transaction (if applicable).

Property ☐ Transaction ☐

PART F — Information about the individual who conducted or proposed to conduct transaction(s) (where applicable)

1. Surname

2. Given name

3. Other/Initial

1A. Alias – Surname

2A. Alias – Given name

3A. Alias – Other/Initial

4. Client number assigned by reporting person or entity (where applicable)

5. Street address

6. City

7. Province or state

8. Country

9. Postal or Zip code

10. Country of residence

11. Home phone number (with area code)

12. Individual's identifier

A ☐ Driver's licence B ☐ Birth certificate C ☐ Provincial health card D ☐ Passport E ☐ Record of Landing or Permanent resident card

F ☐ Other DESCRIPTION (OTHER)

13. ID number (from question 12)

13A. Citizenship

14. Jurisdiction of issue – Country

15. Jurisdiction of issue – Province or state

16. Individual's date of birth

YEAR MONTH DAY

17. Individual's occupation

18. Individual's business phone number (with area code)

18A. Phone extension number

19. Individual's employer

20. Employer's street address

21. Employer's city

22. Employer's province or state

23. Employer's country

24. Postal or Zip code

25. Employer's business telephone number (with area code)

25A. Telephone extension number

NOTE: Please copy this page for each additional disposition (if required).

Property ☐ Transaction ☐ Disposition ☐

PART G — Information about the entity on whose behalf transaction was conducted or proposed to be conducted (where applicable)

1. Name of corporation, trust or other entity

2. Type of business

3. Street address

4. City

5. Province or state

6. Country

7. Postal or Zip code

8. Business phone number (with area code)

8A. Phone extension number

9. Incorporation number (where applicable)

10. Jurisdiction of incorporation – Country

11. Jurisdiction of incorporation – Province or state

12. Individual(s) authorized with respect to the account (up to three (3))

A

B

C

NOTE: Please copy this page for each additional disposition (if required).

Property ☐ Transaction ☐ Disposition ☐

PART H — Information about the individual on whose behalf transaction was conducted or proposed to be conducted (where applicable)

1. Surname

2. Given name

3. Other/Initial

1A. Alias – Surname

2A. Alias – Given name

3A. Alias – Other/Initial

4. Street address

5. City

6. Province or state

7. Country

8. Postal or Zip code

9. Home phone number (with area code)

10. Office phone number (with area code)

10A. Phone extension number

11. Individual's date of birth

YEAR MONTH DAY

12. Individual's identifier

A ☐ Driver's licence B ☐ Birth certificate C ☐ Provincial health card D ☐ Passport E ☐ Record of Landing or Permanent resident card

F ☐ Other

DESCRIPTION (OTHER)

13. ID number (from question 12)

14. Jurisdiction of issue – Country

15. Jurisdiction of issue – Province or state

16. Country of residence

16A. Citizenship

17. Individual's occupation

18. Individual's employer

19. Employer's street address

20. Employer's city

21. Employer's province or state

22. Employer's country

23. Postal or Zip code

24. Employer's business phone number (with area code)

24A. Phone extension number

25. Relationship of the individual named in Part F to the individual named above (fields 1 to 3)

A ☐ Accountant B ☐ Agent C ☐ Legal counsel D ☐ Borrower E ☐ Broker
F ☐ Customer G ☐ Employee H ☐ Friend I ☐ Relative J ☐ Other

DESCRIPTION (OTHER)

The information on this form is collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the *Act*). It will be used for analytical purposes and may also be used for the purposes of ensuring compliance with the Act. Any personal information is protected under the provisions of the *Privacy Act*. For more information, consult http://www.fintrac-canafe.gc.ca/atip-aiprp/infosource-eng.asp.