



Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada

Guideline 6G: Record Keeping and Client Identification for Financial Entities

Guideline 6G: Record Keeping and Client Identification for Financial Entities

July 2016

This replaces the previous version of *Guideline 6G: Record Keeping and Client Identification for Financial Entities* issued in June 2015. The changes made are indicated by a side bar to the right of the modified text in the PDF version.

Table of Contents

1	General	4
2	Record Keeping and Identification Obligations	6
3	Records To Be Kept	8
3.1	General exceptions to record keeping	8
3.2	Large cash transaction records	10
3.3	Records to be kept when opening an account.....	12
3.4	Credit card account records.....	13
3.5	Certain records created in the normal course of business.....	14
3.6	Certain records about the operation of an account.....	15
3.7	Foreign currency exchange transaction tickets.....	15
3.8	Certain transactions of \$3,000 or more	16
3.9	Electronic funds transfers	16
3.10	Trust-related records	18
3.11	Suspicious transaction report records	18
3.12	Identification information on all records	18
4	Client Identity	19
4.1	When and how do you have to ascertain client identity?	19
4.2	General exceptions to client identification.....	20
4.3	Client identity for large cash transactions	22
4.4	Client identity for suspicious transactions	23
4.5	Client identity for signature cards	23
4.6	Client identity for credit card accounts.....	24
4.7	Client identity for electronic funds transfers.....	24
4.8	Client identity for foreign currency exchange transactions.....	25
4.9	Client identity for settlors or co-trustees of a trust.....	25
4.10	Client identity for certain transactions of \$3,000 or more.....	26
4.11	Client identity for group plan account individual members.....	26
4.12	How to ascertain the identity of an individual.....	26
4.13	Client identity for corporations and other entities.....	31
4.14	Keeping client identification information up to date.....	33

5	Ongoing Monitoring of Business Relationship and Related Records ..	33
5.1	Business relationship record.....	37
6	Records about Beneficial Ownership and Control	38
7	Third Party Determination and Related Records	42
7.1	Third party determination.....	42
7.2	Third party records	43
8	Politically Exposed Foreign Person Determination and Related Records	44
8.1	Politically exposed foreign person determination.....	45
8.2	Politically exposed foreign person records	48
9	Correspondent Banking Relationships and Related Records	48
9.1	What is a correspondent banking relationship?	48
9.2	Before you enter into a correspondent banking relationship.....	49
9.3	Correspondent relationship records.....	50
9.4	Confirming identification and other information.....	50
10	Foreign Subsidiaries or Branches	51
11	How Should Records Be Kept?	53
12	Penalties for Non-Compliance	54
13	Comments?	55
14	How to Contact FINTRAC	55

1 General

The objective of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* is to help detect and deter money laundering and the financing of terrorist activities. It is also to facilitate investigations and prosecutions of money laundering and terrorist activity financing offences. This includes reporting, record keeping, client identification and compliance regime requirements for financial entities.

Financial entities are banks (that is, those listed in Schedule I or II of the *Bank Act*) or authorized foreign banks with respect to their operations in Canada, credit unions, caisses populaires, financial services cooperatives, credit union centrals (when they offer financial services to anyone other than a member entity of the credit union central), trust companies, loan companies and agents of the Crown that accept deposit liabilities.

If you are a financial entity, this guideline has been prepared to help you meet your record keeping and client identification obligations, including those for certain foreign subsidiaries or branches. It also contains information about obligations regarding correspondent banking.

This guideline uses plain language to explain the most common situations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as the related Regulations. It is provided as general information only. It is not legal advice, and is not intended to replace the Act and Regulations.

Record keeping and client identification obligations for other types of reporting persons or entities are explained by sector in other versions of this guideline (life insurance companies, brokers and agents; securities dealers; money services businesses; agents of the Crown that sell or redeem money orders; accountants; real estate; dealers in precious metals and stones; British Columbia notaries; and casinos).

For more information about money laundering and terrorist financing, or other requirements under the Act and Regulations applicable to you, see the guidelines in this series:

- *Guideline 1: Background* explains money laundering, terrorist financing, and their international nature. It also provides an outline of the legislative requirements, as well as an overview of FINTRAC's mandate and responsibilities.
- *Guideline 2: Suspicious Transactions* explains how to report a suspicious transaction. It also provides guidance on how to identify a suspicious transaction, including general and industry-specific indicators that may help when conducting or evaluating transactions.
- *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* explains to reporting entities when and how to submit suspicious

transaction reports. There are two different versions of Guideline 3, by reporting method.

- *Guideline 4: Implementation of a Compliance Regime* explains the requirement for reporting entities to implement a regime to ensure compliance with their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations.
- *Guideline 5: Submitting Terrorist Property Reports to FINTRAC* explains to reporting entities when and how to submit terrorist property reports.
- *Guideline 6: Record Keeping and Client Identification* explains the requirement for reporting entities to ascertain the identity of their clients and keep records. There are several different versions of Guideline 6, with each one applicable to a particular sector.
- *Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC* explains when and how to submit large cash transaction reports. There are two different versions of Guideline 7, by reporting method.
- *Guideline 8: Submitting Electronic Funds Transfer Reports to FINTRAC* explains when and how to submit electronic funds transfer reports. There are three different versions of Guideline 8, by type of electronic funds transfer and reporting method.
- *Guideline 9: Submitting Alternative to Large Cash Transaction Reports to FINTRAC* explains when and how financial entities can choose the alternative to large cash transaction reports. This is only applicable to financial entities.
- *Guideline 10: Submitting Casino Disbursement Reports to FINTRAC* explains when and how to submit casino disbursement reports. There are two different versions of Guideline 10, by reporting method.

If you need more help after you read this or other guidelines, call FINTRAC's national toll-free enquiries line at 1-866-346-8722.

Throughout this guideline, several references are provided to additional information that may be available on external websites. FINTRAC is not responsible for the accuracy, reliability or currency of the information contained on those external websites. The links provided are based on information available at the time of publishing of this guideline.

Throughout this guideline, any references to dollar amounts (such as \$10,000) refer to the amount in Canadian dollars or its equivalent in foreign currency. Furthermore, all references to cash mean money in circulation in any country (bank notes or coins). In this context, cash does not include cheques, money orders or other similar negotiable instruments. Also, any references to the term "securities dealer" means an individual or entity authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services.

Your policies and procedures may cover situations other than the ones described in this guideline, for purposes other than your requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. For example, the federal or provincial regulator for your sector may require you to apply additional policies and procedures, the retention period for your records may vary for purposes other than what is described in this guideline, or you may have to request an individual's social insurance number for income tax purposes.

2 Record Keeping and Identification Obligations

As a financial entity, you have the following record keeping and identification obligations.

- When you conduct a large cash transaction, your obligations are as follows:
 - Keep a large cash transaction record (see section 3);
 - Ascertain the identity of the individual (see section 4); and
 - Make third party determinations and keep related records (see section 7).

- When you open an account, other than a credit card account, your obligations are as follows:
 - Keep account opening records (see section 3);
 - Ascertain the identity of clients (see section 4);
 - Make third party determinations and keep related records (see section 7); and
 - Make a determination of whether you are dealing with a politically exposed foreign person and if so, keep records and take other measures (see section 8).

- When you create account operating agreements, debit or credit memos, or client credit files, in the normal course of business, you have to keep those records (see section 3).

- For ongoing account operation, you have to keep certain records and client statements (see section 3).

- When you open a credit card account, your obligations are as follows:
 - Keep credit card account records (see section 3);
 - Ascertain the identity of clients (see section 4); and
 - Make a determination of whether you are dealing with a politically exposed foreign person and if so, keep records and take other measures (see section 8).

- When you conduct certain electronic funds transfers:
 - For an amount of \$1,000 or more, you have to keep a record and ascertain the identity of the client (see sections 3 and 4);

- Include originator information with the transfer (see section 3); and
 - For an amount of \$100,000 or more, you have to make a determination of whether you are dealing with a politically exposed foreign person and if so, take other measures (see section 8).
- When you conduct a foreign exchange transaction, your obligations are as follows:
 - Keep a foreign exchange transaction ticket (see section 3); and
 - Ascertain the identity of the individual if the transaction is for \$3,000 or more (see section 4).
- When you conduct certain transactions of \$3,000 or more with non-account holders, your obligations are as follows:
 - Keep records (see section 3); and
 - Ascertain the identity of the individual (see section 4).
- If you are a trust company, you have additional obligations as follows:
 - Keep records about trusts (see section 3); and
 - Ascertain the identity of the settlors or co-trustees (see section 4).
- When you have to submit a suspicious transaction report to FINTRAC, your obligations include the following:
 - If you have not already ascertained the identity of the individual who conducted or attempted to conduct the transaction, ascertain the identity of the individual (see section 4); and
 - Keep a copy of the report (see section 3).
- When you have to ascertain the identity of your client or confirm the existence of a corporation or other entity, you may have a business relationship with that client. If so, your obligations are as follows:
 - Conduct ongoing monitoring of your business relationship and keep related records (see section 5); and
 - Keep a record of the purpose and intended nature of the business relationship (see section 5).
- If you have to confirm the existence of an entity, you also have to obtain and take reasonable measures to confirm the beneficial ownership information of the entity and keep related records (see section 6).
- Before you enter into a correspondent banking relationship, you have certain obligations. You also have related record keeping obligations (see section 9).
- If you have foreign subsidiaries or branches, you may have obligations regarding them (see section 10).

There are some exceptions and these are explained throughout each section.

The use of personal information in Canadian commercial activities is protected by the *Personal Information Protection and Electronic Documents Act* (PIPEDA), or by substantially similar provincial legislation. You have to inform individuals concerning the collection of personal information about them. However, you do not have to inform individuals when you include personal information about them in any of the reports that you are required to make to FINTRAC. You can get more information about your responsibilities in this area from the following:

- The Office of the Privacy Commissioner of Canada (<http://www.priv.gc.ca>).
 - The Office of the Privacy Commissioner of Canada has developed, on its website, a Question and Answer document entitled *PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (http://www.priv.gc.ca/information/pub/faqs_pcmltfa_01_index_e.asp) that will help you in understanding your responsibilities under both federal laws.

3 Records To Be Kept

As a financial entity, in addition to the records described in sections 5 to 10, you have to keep the following records:

- Large cash transaction records;
- Account opening records;
- Certain records about credit card accounts;
- Certain records created in the normal course of business;
- Certain records about the operation of an account;
- Foreign currency exchange transaction tickets;
- Certain records about transactions of \$3,000 or more;
- Records about electronic funds transfers;
- Trust-related records (trust companies); and
- Suspicious transaction report records.

Details about each of these types of records are provided in subsections 3.2 through 3.11. Also, section 11 explains how your records should be kept.

See section 4 for information about identification requirements that may be associated to the events triggering record keeping requirements.

3.1 General exceptions to record keeping

If you keep information in a record that is already readily available in any other record that you have kept under these rules (as described throughout this guideline), you do not have to keep that information again.

You do not have to keep any of the records described in subsections 3.3 to 3.9, or in section 8, when you open any of the following accounts:

- for the purchase of an immediate or deferred annuity paid for entirely with funds directly transferred from a registered pension plan or the proceeds of a group life insurance policy;
- for the purchase of a registered annuity policy or a registered retirement income fund;
- for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- in the name of an affiliate of a financial entity if the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer;
- for a registered plan, including a locked-in retirement plan, a registered retirement savings plan, a group registered retirement savings plan, a registered education savings plan and any other registered plan;
- an account established pursuant to the escrow requirements of Canadian securities regulators or Canadian stock exchange or any provincial legislation;
- the opening of an account for, or for which instructions are authorized by, a financial entity, a securities dealer, a life insurance company or an investment fund regulated by provincial securities legislation;
- an account opened solely to provide customer accounting services to a securities dealer; or
- where the account holder or settlor is a federally or provincially regulated pension fund.

In addition, you do not have to keep any of the records described in subsections 3.3 to 3.9, or in section 8, for a transaction that is part of a reverse mortgage or structured settlement. This includes opening an account for this type of transaction.

Accounts or transactions for a public body or very large corporation

If you open an account, including a credit card account, or conduct a transaction for a public body or a very large corporation, the record keeping requirements described in subsections 3.3 to 3.9 do not apply. The same is true regarding a subsidiary of either of those entities, if the financial statements of the subsidiary are consolidated with those of the public body or very large corporation.

In this context, a public body means any of the following or their agent:

- a Canadian provincial or federal department or Crown agency;
- an incorporated Canadian municipal body (including an incorporated city, town, village, metropolitan authority, district, county, etc.); or
- a hospital authority. A hospital authority means an organization that operates a public hospital and that is designated to be a hospital authority for GST/HST purposes. For more information on the designation of

hospital authorities, refer to GST/HST Memoranda Series, Chapter 25.2, *Designation of Hospital Authorities* available from the Canada Revenue Agency website (<http://www.cra-arc.gc.ca>) in the forms and publications listed by document type.

Also in this context, a very large corporation is one that has minimum net assets of \$75 million on its last audited balance sheet. The corporation's shares have to be traded on a Canadian stock exchange or on a stock exchange outside Canada that is designated by the Minister of Finance. The corporation also has to operate in a country that is a member of the Financial Action Task Force (FATF). For more information about stock exchanges outside Canada that are designated by the Minister of Finance, refer to the July 2, 2008 news release available in the News area of the Department of Finance's website (<http://www.fin.gc.ca>).

To find out which countries are members of the FATF, refer to its website (<http://www.fatf-gafi.org>).

Credit card acquiring businesses

If you are carrying on activities as a credit card acquiring business, the record-keeping requirements explained in this guideline do not apply to those activities.

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payment for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

3.2 Large cash transaction records

This is a record for every amount of cash of \$10,000 or more that you receive from a client in a single transaction. For example, if your client deposits \$10,000 in cash to an account, you have to keep a large cash transaction record. In addition to this record, a large cash transaction will also require a report to FINTRAC, as explained in *Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC*.

If you know that two or more cash transactions of less than \$10,000 each were made within a 24-hour period (that is, 24 consecutive hours), by or on behalf of the same client, these are considered to be a single large cash transaction if they add up to \$10,000 or more. In this case, you would have to keep a large cash transaction record, and report the transaction to FINTRAC as explained above.

Do **not** keep a large cash transaction record or make a large cash transaction report to FINTRAC if the cash is received from another financial entity or a public body. In this context, a financial entity is one that is included in the description at the beginning of this guideline. For information about what is considered a public body in this context, see information in subsection 3.1 under the heading “Accounts or transactions for a public body or very large corporation.”

Contents of a large cash transaction record

For any large cash transaction, the information you have to keep in a large cash transaction record includes the following:

- the amount and currency of the cash received;
- the date of the transaction;
- the purpose, details and type of transaction (for example, the cash was deposited, or the cash was used to buy traveller’s cheques, etc.) including whether any other individuals or entities were involved in the transaction;
- how the cash was received (for example, in person, by mail, by armoured car, or any other way); and
- if an account was affected by the transaction, include the following:
 - the number and type of any such account;
 - the full name of the client that holds the account; and
 - the currency in which the account’s transactions are conducted.

In the case of a deposit, the large cash transaction record also has to include the following:

- the name of your client in whose account the amount is deposited. If the amount was deposited to more than one client’s account, the record has to include the names of each client; and
- the time of the deposit, if it was made during your normal business hours, or an indication of “night deposit” for any such deposit made outside your normal business hours.

Also, in any case other than a deposit, the large cash transaction record must include the name of the individual from whom you received the cash and that individual’s address and principal business or occupation. This would apply, for example, when you conduct a currency transaction for an individual who is not an account holder. In any case other than a deposit, a large cash transaction record also has to include the individual’s date of birth, whether or not you had to ascertain the identity of that individual.

Be as descriptive as possible regarding the business or occupation. Record information that clearly describes it, rather than use a general term. For example, in the case of a consultant, the occupation recorded should reflect the area of consulting, such as “information technology consultant” or “consulting forester.” As another example, in the case of a professional, the occupation should reflect the nature of the work, such as “petroleum engineer” or “family physician.”

If you have to ascertain the identity of the individual conducting the large cash transaction, see subsection 3.12 for additional information that is required on the large cash transaction record.

3.3 Records to be kept when opening an account

These records are those required when you open an account, **other than a credit card account**. In this context, an account includes one that is for chequing or savings. It also includes an arrangement between you and a client for guaranteed investment certificates, term deposits, mortgages, or other loans.

These records include intended use, signature cards, copies of official corporate records (binding provisions) and other information.

Intended use

For every account you open, you have to keep a record about the account's intended use. This record can also be used when recording the purpose and intended nature of a business relationship. For more information on business relationships, please consult section 5.

Examples of intended use for personal accounts include the following:

- for general cheque services, such as payment of family and household expenses;
- to receive directly deposited employment or pension income;
- to save for eventual payment of children's education;
- to save for retirement;
- to save for a trip, and so on.

Examples of the intended use for commercial accounts include the following:

- for deposits of daily receipts for a business (that is, sales, etc.)
- for payments to employees (payroll);
- for general business operating expenses;
- for payments to suppliers, and so on.

Signature cards

When you open an account, you have to keep a signature card for each account holder. A signature card means any record that is signed by an individual authorized to give instructions for the account. This includes a document such as an application for a deposit account or a mortgage.

In the case of group plan accounts, you do **not** have to keep a signature card for any individual member of the plan if the plan's sponsor is an entity and you have already confirmed its existence. However, unless the plan is exempt from record keeping requirements as explained in subsection 3.1, you have to keep a signature card for each individual member for whom a contribution is made that is other than a contribution made by payroll deductions or by the plan's sponsor.

If you have to ascertain the identity of the individual signing the signature card, see subsection 3.12 for additional information required on that record.

Accounts for corporations

If the account is opened for a corporation, you have to keep a copy of the part of the official corporate records showing the provisions that relate to the power to bind the corporation regarding the account. This could be a certificate of incumbency, the articles of incorporation or the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc. If there were changes subsequent to the articles or bylaws that relate to the power to bind the corporation regarding the account and these changes were in effect at the time the account was opened, then the board resolution stating the change would be included in this type of record.

Accounts for individuals or entities other than corporations

If the account is opened for an individual or an entity that is not a corporation, you have to keep a record of the name, address and principal business or occupation of that individual or entity. For more information about recording business or occupation, see subsection 3.2, under the heading “Contents of a large cash transaction record.” If the record is about an individual, it also has to include the individual’s date of birth.

3.4 Credit card account records

You have to keep the following records relating to credit card accounts.

All credit card accounts

When you open any credit card account, you have to keep a record of the name, address, telephone number and date of birth of every holder of a credit card for that account. For the date of birth, you have to take reasonable measures to obtain it, such as asking the credit card account applicant for it.

You also have to keep the following records in relation to the credit card account:

- every credit card application that you receive from a client in the normal course of business; and
- a copy of every credit card statement that you send to a client (unless that information is readily available in other records you keep under these rules).

Credit card accounts for individuals

When you open a credit card account for an individual, you also have to keep a record about that individual’s name, address, date of birth and principal business or occupation. For more information about recording business or occupation, see subsection 3.2, under the heading “Contents of a large cash transaction record.”

Credit card accounts for entities

When you open a credit card account for a corporation, you also have to keep a copy of the official corporate records that contain any provision relating to the power to bind the corporation in respect of the account. See subsection 3.3, under the heading “Accounts for corporations,” for more information about this.

If the credit card account is for an entity other than a corporation, you also have to record its name, address and principal business.

3.5 Certain records created in the normal course of business

You have to keep the following records that you create in the normal course of business with a client. These do not apply for credit card accounts.

Account operating agreement

An account operating agreement is any document you create in the normal course of business that outlines the agreement between you and your client about the account’s operation. For example, an application for a deposit account or a mortgage can include a reference to a separate document setting out the terms and conditions of the account’s operation. The account operating agreement record in that case would include both the application and the separate document.

Debit or credit memos

You have to keep any debit or credit memo that you create or receive in the normal course of business regarding an account. This does not apply to debit memos that relate to another account at the same branch.

Client credit files

A client credit file means a record you create in the normal course of business that relates to a credit arrangement with your client, such as a mortgage, loan or other type of credit agreement. This includes your client’s name, address and financial capacity as well as the terms of credit. It also includes your client’s principal business or occupation, the name of the business (if any), and your client’s business address or place of work address. For more information about recording business or occupation, see subsection 3.2, under the heading “Contents of a large cash transaction record.”

Client credit files include credit applications that were declined. This also includes cancelled credit applications unless the application was cancelled before it was considered by the financial entity.

3.6 Certain records about the operation of an account

You have to keep the following records relating to the operation of an account:

- a copy of every **account statement** that you send to your client. If the information in an account statement is readily available in other records that you have to keep (as described throughout section 3), it does not have to be kept again.
- a **deposit slip** for every deposit made to an account. A deposit slip means a record that sets out the date of a deposit, the amount of the deposit, and any part of it that was made in cash. A deposit slip also sets out the holder of the account in whose name the deposit is made and the number of the account.
- every **cleared cheque** drawn on or deposited to an account. This does not apply to cheques if they are drawn on and deposited to accounts at the same branch. It does not apply either if you have electronic or microfilm records that are retained for at least five years and that can readily reproduce images of the cheques.

3.7 Foreign currency exchange transaction tickets

For every foreign currency exchange transaction you conduct, regardless of the amount, you have to keep a transaction ticket. A transaction ticket means a record that sets out the following information:

- the date, amount and currency of the purchase or sale; and
- the method, amount and currency of the payment made or received.

A transaction ticket can take the form of an entry in a transaction register, as long as it contains the information required, as explained in this subsection.

If the transaction was \$3,000 or more, the foreign currency exchange transaction ticket also has to set out the name, address and date or birth of the individual who carried out the transaction.

If you have to ascertain the identity of the individual conducting the foreign currency exchange transaction, see subsection 3.12 for additional information that is required on the transaction ticket.

3.8 Certain transactions of \$3,000 or more

You have to keep records for every one of the following transactions that you conduct with an individual or entity. This applies whether or not they are an account holder.

- If you receive \$3,000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments, keep a record of the date, the amount received and the name and address of the individual who gave you the amount. These records also must indicate whether the amount was received in cash, cheques, traveller's cheques, money orders or other similar negotiable instruments.

However, if you receive \$3,000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments from a financial entity, you do not have to keep the record described above.

- If you redeem \$3,000 or more in money orders, whether it is one money order or two or more taken together, keep a record of the date as well as the name and address of the individual redeeming them. These records also must indicate the name of the issuer of each money order.

If you have to ascertain the identity of the individual conducting any of these types of transaction, see subsection 3.12 for additional information that is required on the record.

3.9 Electronic funds transfers

Information to include with outgoing transfers

If you **send** an electronic funds transfer (EFT) of any amount, at the request of a client, you have to include **originator information** with the transfer. Originator information means the name, address and, if any, the account number or reference number of the client who requested the transfer. You should not send any EFTs without including originator information.

An EFT means the transmission—through any electronic, magnetic or optical device, telephone instrument or computer—of instructions for the transfer of funds to or from Canada. In the case of messages sent through the SWIFT network, only SWIFT MT 103 messages are included. In addition, only in the context of subsections 3.9 and 4.7 of this guideline, an EFT includes any transmission of instructions for the transfer of funds **within Canada** that is a SWIFT MT 103 message.

An EFT does **not** include the following transactions:

- that use credit or debit cards, when the recipient has an agreement with the payment service provider for the payment of goods and services;

- where the recipient withdraws cash from their account;
- that use direct deposits or pre-authorized debits; or
- that use cheque imaging and presentment.

The exceptions described in subsection 3.1 do not apply to these requirements regarding originator information.

Information to be included with incoming transfers

If you **receive** an EFT, you have to take reasonable measures to ensure it includes originator information. In this context, reasonable measures could include contacting the institution that sent the payment instructions.

These requirements apply to the same EFTs as described above under the heading “Information to include with outgoing transfers,” with the same exclusions. Also, as explained above, the exceptions described in subsection 3.1 do not apply to these requirements regarding originator information.

EFT record

If you **send** an EFT in an amount of \$1,000 or more, you have to keep a record. In this context, an EFT is as described above under the heading “Information to include with outgoing transfers,” with the same exclusions.

The EFT record has to include the following:

- if the client is an individual, the individual’s name, address, date of birth and telephone number as well as the nature of their principal business or occupation;
- if the client is an entity, the name, address, date of birth and telephone number of the individual who initiated the transaction on behalf of the entity, as well as the nature of the individual’s principal business or occupation;
- the relevant account number, if any, the reference number, if any, and the date of the transaction;
- the name or account number of the individual or entity to whom the amount is sent; and
- the amount and currency of the transaction.

For more information about recording business or occupation, see subsection 3.2, under the heading “Contents of a large cash transaction record.”

The requirement for this record does **not** apply to incoming funds transfers.

If you have to ascertain the identity of the individual initiating the transfer, see subsection 3.12 for additional information that is required on the EFT record.

If the EFT involved an exchange to or from a foreign currency, see subsection 3.7 for additional information required in a transaction ticket.

3.10 Trust-related records

If you are a trust company (that is, the *Trust and Loan Companies Act* applies to you, or you are regulated by a provincial Act), in addition to the records explained throughout section 3, you also have to keep the following records about every trust for which you are trustee:

- a copy of the trust deed; and
- a record of the settlor's name, address and principal business or occupation. If the settlor is an individual, the record also has to include the settlor's date of birth.

For more information about recording business or occupation, see subsection 3.2, under the heading "Contents of a large cash transaction record." In addition, see subsection 3.12 for additional information that is required on records about settlors if the settlors are individuals and you have to ascertain their identity.

If the trust is an institutional trust and the settlor is a corporation, in addition to the record keeping requirements described above you have to keep a copy of the part of the official corporate records showing the provisions that relate to the power to bind the corporation regarding the trust. An institutional trust is one that is established by a corporation, a partnership or other entity. It includes pension plan trusts, pension master trusts, supplemental pension plan trusts, mutual fund trusts, pooled fund trusts, registered retirement savings plan trusts, registered retirement income fund trusts, registered education savings plan trusts, group registered retirement savings plan trusts, deferred profit sharing plan trusts, employee profit sharing plan trusts, retirement compensation arrangement trusts, employee savings plan trusts, health and welfare trusts, unemployment benefit plan trusts, foreign insurance company trusts, foreign reinsurance trusts, reinsurance trusts, real estate investment trusts, environmental trusts and trusts established in respect of endowments, foundations and registered charities.

3.11 Suspicious transaction report records

When you have to report a suspicious transaction to FINTRAC, you have to keep a copy of the report. See *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* for more information about obligations related to this report.

3.12 Identification information on all records

If you have to ascertain the identity of an individual, as explained in section 4, in association with any of the records mentioned in section 3, you have to keep the individual's name with that record. You also have to keep the following with that record:

Identification documents

If you have to ascertain the identity of the individual using an identification document, the record has to include the type of document you used to confirm the individual's identity, its reference number and its place of issue.

Identification of clients not physically present

If you do not use an identification document but use methods for a client who is not physically present (as described in subsection 4.12), you have to include whichever of the following, according to the methods used:

- If you use a cleared cheque to ascertain the individual's identity, the record has to include the name of the financial entity and the account number of the deposit account on which the cheque was drawn;
- If you confirm that the individual holds a deposit account with a financial entity, the record has to include the date on which you made the confirmation as well as the name of the financial entity where the account is held and the number of the account;
- If you rely on a previous confirmation of the individual's identity by an affiliate of yours or another member of your central cooperative credit society, the record has to include the name of that other entity as well as the type and reference number of the record that they previously relied on to ascertain the individual's identity;
- If you use an identification product, the record has to include the name of the identification product, the name of the entity offering it, the search reference number and the date you used the product to ascertain the individual's identity;
- If you consult a credit file, the record has to include the name of the entity keeping the credit file and the date you consulted it;
- If you use an attestation signed by a commissioner of oaths in Canada or a guarantor in Canada, you have to keep the attestation;
- If you consult an independent data source, the record has to include the name of the data source, the date you consulted it and the information it provided;
- If you rely on a utility invoice issued in the individual's name, you have to keep the invoice or a legible photocopy or electronic image of it;
- If you rely on a photocopy or electronic image of an identification document provided by the individual, you have to keep that photocopy or electronic image; and
- If you rely on a deposit account statement for the individual, you have to keep a legible photocopy or electronic image of it.

4 Client Identity

4.1 When and how do you have to ascertain client identity?

As a financial entity, you have client identification obligations. You have to take the following measures to ascertain the identity of individuals or to confirm the

existence of entities (entities meaning: corporations, trusts, partnerships, funds, and unincorporated associations or organizations), subject to the general exceptions in subsection 4.2.

If you cannot ascertain the identity of an individual or confirm the existence of an entity when you open an account according to the identification requirements, you cannot open the account. This means that no transaction other than an initial deposit can be carried out unless you are able to ascertain the identity of the individual or entity as explained throughout section 4. As well, if you suspect that the transaction is related to a money laundering or terrorist financing offence, you must file a suspicious transaction report, as explained in *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC*.

Subsections 4.3 to 4.11 explain the need to ascertain the identity of an individual when an event triggers the requirement. In these events, you must ascertain the identity of an individual, unless an exception applies as explained in subsection 4.2.

Refer to section 3 for information about record keeping requirements that may be associated to the events triggering identification requirements.

Once you have conducted two transactions with a client that require you to ascertain the identity of the client, you have entered into a business relationship with that client. See section 5 for more information on business relationships and related records.

4.2 General exceptions to client identification

In addition to the exceptions explained throughout the rest of section 4, the following general exceptions apply to client identification requirements:

Existing clients

Once you have ascertained the identity of an individual as explained in this guideline, you do not have to ascertain their identity again if you **recognize the individual** (visually or by voice) at the time of a future event that would otherwise trigger the identification requirement. However, if you have any doubts about the identification information previously collected, you will have to ascertain that individual's identity again. For example, you could have doubts if the identification information does not match the physical description of the individual.

Once you have confirmed the existence of a corporation and confirmed its name, address and the names of its directors (as explained in subsection 4.13), you are not required to confirm that same information in the future.

Once you have confirmed the existence of an entity other than a corporation (as explained in subsection 4.13), you are not required to confirm that same information in the future.

You do not have to ascertain the identity of an individual as described in subsections 4.5 to 4.10, nor do the requirements described in subsection 8.1 for new accounts apply:

- for an individual who already has an account with you; or
- if you are an entity and you open an account for the deposit by a life insurance company of a death benefit under a life insurance policy or annuity. In order for this exception to apply, you have to be affiliated with the life insurance company opening the account and the following conditions have to be met:
 - the account is opened for a beneficiary that is an individual;
 - only that death benefit may be deposited into the account; and
 - the policy or annuity contract, under which the death benefit claim was made, has been in existence for at least two years before the day on which the death benefit claim was made.

In this context, the life insurance company is affiliated with the entity if one fully owns the other if they are both owned by the same other entity or if their financial statements are consolidated.

Certain types of accounts or transactions

You do not have to ascertain the identity of an individual as described in subsection 4.5 at the opening of a business account for which you have already identified three persons who are authorized to give instructions in respect of the account.

You do not have to ascertain the identity of clients as described in subsections 4.5 to 4.11 and subsection 4.13, nor do the requirements described in sections 5, 6 or 8 apply, in the following situations:

- the opening of an account for the purchase of an immediate or deferred annuity paid for entirely with funds directly transferred from a registered pension plan or the proceeds of a group life insurance policy;
- the opening of an account for the purchase of a registered annuity policy or a registered retirement income fund;
- any transaction, including opening an account for the transaction, that is part of a reverse mortgage or structured settlement;
- the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- the opening of an account in the name of an affiliate of a financial entity if the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer;
- the opening of an account for a registered plan, including a locked-in retirement plan, a registered retirement savings plan, a group registered

retirement savings plan, a registered education savings plan, or any other registered plan;

- the opening of an account established pursuant to the escrow requirements of Canadian securities regulators or Canadian stock exchange or any provincial legislation;
- the opening of an account for, or for which instructions are authorized by, a financial entity, a securities dealer, a life insurance company or an investment fund regulated by provincial securities legislation;
- the opening of an account solely to provide customer accounting services to a securities dealer; or
- the opening of an account where the account holder or settlor is a federally or provincially regulated pension fund.

Accounts or transactions for a public body or very large corporation

If you open an account, including a credit card account, or conduct a transaction for a public body or a very large corporation, the requirements described in subsections 4.5 to 4.10 or section 6, do not apply. The same is true regarding a subsidiary of either of those entities, if the financial statements of the subsidiary are consolidated with those of the public body or very large corporation.

For information about what is considered a public body or a very large corporation in this context, see subsection 3.1 under the heading “Accounts or transactions for a public body or very large corporation.”

Credit card acquiring businesses

If you are carrying on activities as a credit card acquiring business, client identification requirements do not apply to those activities. For information about what a credit card acquiring business means, see subsection 3.1.

4.3 Client identity for large cash transactions

You have to ascertain the identity of any individual with whom you conduct a large cash transaction, at the time of the transaction, if you have to keep a large cash transaction record for it, as described in subsection 3.2. If the transaction is a deposit to a business account (including a quick drop or night deposit) or through an automated banking machine, you do not have to ascertain the identity of the individual conducting it.

As explained in subsection 4.2, once you have ascertained the identity of an individual, you do not have to ascertain their identity again if you recognize the individual. None of the other exceptions explained in subsection 4.2 apply in the case of large cash transactions.

See subsection 4.12 to find out how to ascertain the identity of an individual for a large cash transaction.

4.4 Client identity for suspicious transactions

When you have to send a suspicious transaction report to FINTRAC, you have to take reasonable measures, before the transaction is reported, to ascertain the identity of the individual who conducted or attempted to conduct the transaction.

This does not apply in the following circumstances:

- if you had already ascertained the identity of the individual as required and you have no doubts about that previous identification information; or
- if you believe that doing so would inform the individual that you are submitting a suspicious transaction report.

In this context, reasonable measures to ascertain the identity of an individual include using either Option 1 or Option 2 as explained in subsection 4.12 under the heading “Individual not physically present.” They also include asking the individual for an identification document. However, reasonable measures exclude any method that you believe would inform the individual that you are submitting a suspicious transaction report.

It is important to remember that all suspicious transactions and attempted transactions, including transactions that are normally exempt from client identification requirements, require you to take reasonable measures to ascertain your client’s identity. See *Guideline 2: Suspicious Transactions* for more information.

4.5 Client identity for signature cards

You have to ascertain the identity of any individual who signs a signature card for an account that you open (other than a credit card account) before any transaction (other than the initial deposit) is carried out. In cases where a business account has more than three individuals authorized for it, you have to ascertain the identity of at least three of those individuals.

If the individual who signs a signature card is under 12 years old, ascertain the identity of the individual’s father, mother or guardian before any transaction (other than the initial deposit) is carried out.

If you open an account for an entity, there are identification requirements in addition to the one regarding signature cards. Refer to subsection 4.13 for more information about this.

See subsection 4.12 to find out how to ascertain the identity of an individual for a signature card.

4.6 Client identity for credit card accounts

Credit card accounts for individuals

You have to ascertain the identity of any individual who opens a credit card account, before any credit card is activated for the account. If there are credit cards issued for the account that are for individuals other than the individual opening the account, you have to record information about them (as explained in subsection 3.4), but you do not have to ascertain their identity. For example, a mother applying for a credit card account requests that a credit card be issued on that account for her son and daughter. In this example, the mother's identity has to be ascertained as she is the account holder, but the identity of the son and daughter does not.

If there are two or more co-applicants for a credit card account (in other words, if a credit card account is opened in the name of more than one individual), the identification requirement applies to all co-applicants.

See subsection 4.12 to find out how to ascertain the identity of an individual for a credit card account.

Credit card accounts for entities

When you open a credit card account for a corporation, you have to confirm the corporation's existence and find out its name and address as well as its directors' names. However, if you open a credit card account for a corporation that is a securities dealer, you do not need to find out its directors' names.

If the credit card account is for an entity other than a corporation, you have to confirm that entity's existence.

See subsection 4.13 for more information about client identity for corporations and other entities. These requirements have to be met before any credit card is issued on the account.

4.7 Client identity for electronic funds transfers

You have to ascertain the identity of any individual who requests an electronic funds transfer (EFT) of \$1,000 or more, at the time of the transaction. This does **not** apply if that individual has signed a signature card for an account with you or is authorized to act regarding such an account.

An EFT means the transmission—through any electronic, magnetic or optical device, telephone instrument or computer—of instructions for the transfer of funds to or from Canada. In the case of messages sent through the SWIFT network, only SWIFT MT 103 messages are included. In addition, in the context of subsections 3.9 and 4.7 only, an EFT includes any transmission of instructions for the transfer of funds **within Canada** that is a SWIFT MT 103 message.

An EFT does **not** include to the following transactions:

- that use credit or debit cards, when the recipient has an agreement with the payment service provider for the payment of goods and services;
- where the recipient withdraws cash from their account;
- that use direct deposits or pre-authorized debits; or
- that use cheque imaging and presentment.

This identification requirement does **not** apply to incoming funds transfers.

See subsection 4.12 to find out how to ascertain the identity of an individual for a funds transfer.

4.8 Client identity for foreign currency exchange transactions

You have to ascertain the identity of any individual who conducts a foreign currency exchange transaction of \$3,000 or more at the time of the transaction. This does **not** apply if that individual has signed a signature card for an account with you or is authorized to act regarding such an account.

See subsection 4.12 to find out how to ascertain the identity of an individual for a foreign currency exchange transaction.

4.9 Client identity for settlors or co-trustees of a trust

The following requirements to ascertain the identity of individuals and confirm the existence of entities apply to you if you are a **trust company** and you are the **trustee** for a trust.

Individuals

You have to ascertain the identity of the following individuals:

- any individual who is the settlor of a personal trust (other than a trust created by a will) if the trust is one for which you have to keep a record described in subsection 3.10.
- any individual who is authorized to act as co-trustee of any trust.

In both cases, you have to do this within 15 days of becoming the trustee.

If an entity is authorized to act as a co-trustee of a trust, you also have to ascertain the identity of the individuals (up to three of them) authorized to give instructions on behalf of the entity's activities as a co-trustee. This also has to be done within 15 days of becoming the trustee.

See subsection 4.12 to find out how to ascertain the identity of an individual relating to a trust.

Entities

If you are a trust company, you have to confirm the existence of any entity that is the settlor of an institutional trust, or that is authorized to act as a co-trustee of any trust. You have to do this within 15 days of becoming the trustee. As explained above, under the heading “Individuals,” in cases where an entity is authorized to act as a co-trustee of any trust, you also have to ascertain the identity of the individuals authorized to give instructions for that entity’s activities as co-trustee.

As explained in subsection 4.2, the requirement to confirm the existence of an entity does not apply for the opening of an account if the settlor of the trust is a federally or provincially regulated pension fund.

To find out how to confirm the existence of a **corporation**, read the information in subsection 4.13, under the heading “Corporations.” To find out how to confirm the existence of an **entity other than a corporation**, read the information in subsection 4.13 under the heading “Entities other than corporations.”

4.10 Client identity for certain transactions of \$3,000 or more

You have to ascertain the identity of any individual for whom you issue or redeem traveller’s cheques, money orders or other similar negotiable instruments for \$3,000 or more. This does **not** apply if that individual has signed a signature card for an account with you or is authorized to act regarding such an account.

If you are required to ascertain the identity of an individual in any of these cases, you have to do so at the time of the transaction.

See subsection 4.12 to find out how to ascertain the identity of an individual for this purpose.

4.11 Client identity for group plan account individual members

In the case of a group plan account that is not exempt from identification requirements as explained in subsection 4.2, you have to ascertain the identity of any individual members for whom you have to keep a signature card as explained in subsection 3.3 under the heading “Signature cards.” In this case, you have to ascertain the identity of the individual members when they make contributions to the plan.

4.12 How to ascertain the identity of an individual

See subsection 3.12 for additional information that is required on certain records when you have to ascertain the identity of individuals.

To ascertain the identity of an individual for the requirements described in this guideline, refer to one of the following: the individual's birth certificate, driver's licence, passport, record of landing, permanent resident card or other similar document.

You can refer to an individual's provincial health card, but only if it is not prohibited by provincial or territorial legislation. For example, you cannot refer to an individual's provincial health card from Ontario, Manitoba, Nova Scotia or Prince Edward Island since health cards cannot be used for this purpose in these provinces. As another example, in Quebec, you cannot request to see a client's health card, but you may accept it if the client wants to use it for identification purposes. If you have questions about the use of health cards for identification, please contact the appropriate provincial issuer for more information.

For a document to be acceptable for identification purposes, it must have a unique identifier number. Also, the document must have been issued by a provincial, territorial or federal government. For example, a birth or baptismal certificate issued by a church would not be acceptable for this purpose. Also, an identification card issued by an employer for an employee (that is, an employee identification card) is not acceptable.

The document also has to be a valid one and cannot have expired. For example, an expired driver's licence would not be acceptable.

A social insurance number (SIN) card can be used to ascertain the identity of a client, but the SIN (that is, the number itself) is not to be provided to FINTRAC on any type of report. The Office of the Privacy Commissioner (<http://www.priv.gc.ca>) has produced a fact sheet concerning best practices for the use of SINs. Please consult it for more information on this topic.

Examples of other documents that can be used to ascertain the identity of a client include a certificate of Indian status or a provincial or territorial identification card issued by any of the following (or their successors):

- the Insurance Corporation of British Columbia;
- Alberta Registries;
- Saskatchewan Government Insurance;
- the Department of Service Nova Scotia and Municipal Relations;
- the Department of Transportation and Public Works of the Province of Prince Edward Island;
- Service New Brunswick;
- the Department of Government Services and Lands of the Province of Newfoundland and Labrador;
- the Department of Transportation of the Northwest Territories; or
- the Department of Community Government and Transportation of the Territory of Nunavut.

Valid foreign identification, if equivalent to an acceptable type of Canadian identification document, would also be acceptable for the purposes explained in this guideline. For example, a valid foreign passport is acceptable.

When you refer to a document to ascertain the identity of an individual, it has to be an original, not a copy of the document. In cases where it is not possible for you to view the original yourself, you may choose to use an agent or mandatary to verify the original identification document on your behalf. Even if you use an agent or mandatary, you are responsible for making sure the identification requirements are met.

Use of an agent or mandatary

If you use an agent or mandatary to meet your client identification obligations, you have to enter into a written agreement or arrangement with the agent or mandatary outlining what you expect them to do for you. In addition, you have to obtain from the agent or mandatary the customer information that was obtained according to the agreement or arrangement. The agent or mandatary can be any individual or entity, as long as you meet these two conditions regarding written agreement and obtaining customer information.

Your agent or mandatary can ascertain the identity of your client for you using an identification document. In cases where your client is not physically present at the opening of an account, establishment of a trust or conducting of a transaction, your agent or mandatary can also use the options explained below.

Individual not physically present

If you have to ascertain the identity of an individual who is **not physically present** you have to use one or the other of the following options:

OPTION 1: Affiliate or co-member

To ascertain the identity of an individual using this option, you have to first obtain the individual's name, address and date of birth. Then, you have to confirm that one of the following has ascertained the identity of the individual by referring to an original identification document:

- a financial entity, life insurance company or securities dealer affiliated with you;
- an entity affiliated with you and whose activities outside Canada are similar to those of a financial entity, life insurance company or securities dealer; or
- another financial entity that is a member of your financial services cooperative association or credit union central association of which you also are a member.

To use this option, you have to verify that the individual's name, address and date of birth provided to you correspond with the information kept in the records of that other entity.

In this context, an entity is affiliated with you if you fully own it or it fully owns you, or you are both fully owned by the same entity.

OPTION 2: Combination of methods

To ascertain the identity of an individual using this option, you have to use a combination of **two** of the following methods. In each of the two methods you use, the individual's information has to be consistent with what you have in your records. The information also has to be consistent from one method to the other. For example, if each of the methods you use has the name, address and date of birth information about the individual, all of it has to agree with what you have in your records.

The methods below may not apply for all clients. For example, the methods would not be available to ascertain the identity of a client outside Canada who is opening an account with you, but has no Canadian credit history, no access to a Canadian guarantor and no deposit account with a financial entity. In this case, ascertaining the identity of the client using an identification document may necessitate the use of an agent or mandatary, as explained above.

Identification product or credit file method

You can use the following methods:

- Refer to an independent and reliable identification product. It must be based on personal information as well as Canadian credit history about the individual of at least six months duration. This type of product can use a series of specific questions, based on an individual's credit file, to help you ascertain client identity.
- With the individual's permission, refer to a credit file. The credit file must have been in existence for at least six months.

If you are ascertaining the identity of an individual for a credit card account, you can combine the identification product and credit file methods. Otherwise, these methods cannot be combined.

Products for either of these methods are available commercially, such as those used for credit ratings.

Attestation method

Obtain an attestation that an original identification document for the individual has been seen by a commissioner of oaths or a guarantor. The attestation must be on a legible photocopy of the document and include the following information:

- the name, profession and address of the commissioner of oaths or the guarantor;
- the signature of the commissioner of oaths or the guarantor; and

- the type and number of the identifying document provided by the individual whose identity you must ascertain.

In this context, a guarantor has to be an individual engaged in one of the following professions in Canada:

- a dentist, a medical doctor or a chiropractor;
- a judge, a magistrate or a lawyer;
- a notary (in Quebec) or a notary public;
- an optometrist or a pharmacist;
- an accredited public accountant (APA), a chartered accountant (CA), a certified general accountant (CGA), a certified management accountant (CMA), a public accountant (PA) or a registered public accountant (RPA);
- a professional engineer (P. Eng., in a province other than Quebec) or engineer (Eng. in Quebec); or
- a veterinarian.

Cleared cheque or deposit account method

You can use the following methods.

- Confirm that a cheque drawn on a deposit account that the individual has with a financial entity has cleared. This means a cheque that was written by the individual, cashed by the payee and cleared through the individual's account. It does not include pre-authorized payments as these are not cheques written by the individual.
- Confirm that the individual has a deposit account with a financial entity.

If you are ascertaining the identity of an individual for a credit card account, you can combine the cleared cheque and deposit account methods. Otherwise, these methods cannot be combined.

If you use the cleared cheque or deposit account method, the account cannot be one that is exempt from identification requirements as explained in subsection 4.2 under the headings "Certain types of accounts or transactions" and "Accounts or transactions for a public body or very large corporation."

A financial entity is one that is included in the description at the beginning of this guideline. This means that a deposit account can be used in either of these methods as long as it is with a bank listed in Schedule I or II of the *Bank Act*, an authorized foreign bank with respect to its operations in Canada, a credit union, a caisse populaire, a trust and loan company or an agent of the Crown that accepts deposit liabilities. In the case of a foreign bank, the deposit account has to be in Canada. Financial entities

also include financial services cooperatives and credit union centrals as explained in section 1.

Additional methods available only for credit card accounts

If you have to ascertain the identity of an individual who is not physically present at the opening of a credit card account, you can use either option 1 or option 2 as described above. For option 2, additional methods are available as follows:

- Consult a reputable, independent data source that is compiled from a telecommunications directory. It must contain the names, addresses and telephone numbers of individuals to confirm the individual's name, address and telephone number.
- If you are ascertaining the identity of an individual credit card applicant who has no credit history in Canada, for a credit limit of no more than \$1,500, the available methods also include the following:
 - Obtain a utility invoice issued by a Canadian utility in the name of the individual and that includes the individual's address.
 - Obtain a legible photocopy or an electronic image of an identification document for the individual.
 - Obtaining a legible photocopy or an electronic image of a deposit account statement issued by a financial entity in the name of the individual.

4.13 Client identity for corporations and other entities

You have to confirm the existence of any corporation or other entity for which you open an account, other than a credit card account, before any transaction other than the initial deposit, is conducted. For a credit card account, as explained in subsection 4.6, you have to confirm the existence of the entity before any credit card is issued on the account.

In the case of a corporation, in addition to confirming its existence, you also have to determine the corporation's name, address and the names of its directors.

If you are a trust company, you have to confirm the existence of any corporation or other entity that is the settlor of an institutional trust for which you have to keep records (as explained in subsection 3.10). The same is true for any corporation or other entity that is a co-trustee. See subsection 4.9 for more information. In the case of any identification of a corporation as a settlor or co-trustee, you do not have to determine the names of the corporation's directors.

When you have to confirm the existence of an entity, you also have to obtain and take reasonable measures to confirm the entity's beneficial ownership, as explained in section 6.

Corporations

To confirm the existence of a corporation as well as the corporation's name and address, refer to the following documents:

- the corporation's certificate of corporate status;
- a record that has to be filed annually under provincial securities legislation; or
- any other record that confirms the corporation's existence. Examples of these include such other records as the corporation's published annual report signed by an independent audit firm, or a letter or a notice of assessment for the corporation from a municipal, provincial, territorial or federal government.

You also have to determine the names of the corporation's directors (except in the case of identification of a corporation as a settlor or co-trustee, as explained above). To do this, you may need to see the list of the corporation's directors submitted with the application for incorporation. If you open an account for a corporation that is a securities dealer, you do not need to determine the name of the corporation's directors.

The record you use to confirm a corporation's existence can be a paper or an electronic version. Although such information may be available verbally (such as by phone), it is not acceptable for these purposes, as you have to refer to a record. If the record is in paper format, you have to keep the record or a copy of it.

If the record is an electronic version, you have to keep a record of the corporation's registration number, the type and source of the record. An electronic version of a record has to be from a public source. For example, you can get information about a corporation's name and address and the names of its directors from a provincial or federal database such as the Corporations Canada database which is accessible from Industry Canada's website (<http://www.ic.gc.ca>). As another example, you may also get this type of information if you subscribe to a corporation searching and registration service.

Entities other than corporations

In the case of an entity other than a corporation, refer to a partnership agreement, articles of association or any other similar record that confirms the entity's existence. The record you use to confirm the existence of an entity can be paper or an electronic version. Although such information may be available verbally (such as by phone), it is not acceptable for these purposes, as you have to refer to a record. If the record is in paper format, you have to keep the record or a copy of it.

If the record is an electronic version, you have to keep a record of the entity's registration number, the type and source of the record. An electronic version of a record has to be from a public source.

4.14 Keeping client identification information up to date

Your compliance regime has to include an assessment, in the course of your activities, of the risk of money laundering or terrorist financing. *Guideline 4: Implementation of a Compliance Regime* provides more information about risk assessment requirements. According to this assessment, you have to keep client identification information up to date as part of your ongoing monitoring obligations.

Measures to keep client identification information up to date include asking the client to provide information to confirm or update their identification information. In the case of an individual client, this can also include confirming or updating the information by using the same options that are available to ascertain the identity of individuals who are not physically present.

In the case of clients that are entities, measures to keep client identification information up to date include consulting a paper or electronic record as explained in subsection 4.13, or obtaining information verbally.

The frequency with which client identification information is to be kept up to date will vary depending on your risk assessment of your client. As part of your ongoing monitoring obligations, you have to keep all client identification information up to date. For high-risk clients, you must update client identification information more frequently and perform more frequent monitoring, as well as adopt any other appropriate enhanced monitoring measures (see examples in section 5).

If you have used one of the exceptions found in 4.2 (General exceptions to client identification) where you were not required to ascertain the identity of a client and therefore, do not have any client information in your records, there will be no client information to update as part of your ongoing monitoring obligations as described in section 5 (Ongoing Monitoring of Business Relationship and Related Records), but your other ongoing monitoring obligations still apply.

5 Ongoing Monitoring of Business Relationship and Related Records

Business relationship

A business relationship is a relationship that you establish with a client to conduct financial transactions or provide services related to those transactions.

For financial institutions, these relationships can be established within or outside of an account.

If you are carrying on activities as a credit card acquiring business, business relationship requirements do not apply to those activities. For more information on credit card acquiring businesses, see subsection 3.1.

Account-based business relationship: You are in a business relationship with a client that holds an account with you. You enter into a business relationship when a client opens an account with you. For a new or existing client that has one or more accounts, the business relationship includes all transactions and activities relating to those accounts.

Non-account-based business relationship: If your client does not have an account, you enter into a business relationship when you conduct two or more transactions in which you have to:

- ascertain the identity of the individual (see section 4); or
- confirm the existence of a corporation or other entity (see sections 4 and 6).

In such a case, the business relationship only includes transactions and related activities for which you have to ascertain the identity of your client. See section 4 for more information on these transactions and activities.

If you use the exception to ascertaining the identity of a client where you recognize the individual (as described in 4.2 General exceptions to client identification) in the case of a second transaction that requires you ascertain the identity of a client, you have entered into a business relationship with that client nonetheless. This is because it is the requirement to ascertain identity that triggers the business relationship.

You should determine that a business relationship has been established as soon as reasonably practicable following the second transaction requiring that the client's identity be ascertained. As a best practice, this should be done within 30 calendar days.

If you have a client without an account who conducts two or more suspicious transactions, you have still entered into a business relationship with that client, even if you are unable to ascertain the identity of that client. This is because suspicious transactions require you to take reasonable measures to ascertain the identity of the client (subject to the circumstances described in section 4.4), and so two or more of these transactions will trigger a business relationship. You 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 (see examples under "Ongoing monitoring" below).

A business relationship is established when two transactions that require you to ascertain the identity of your client occur within a maximum of five years from one another. If a period of five years passes from the last transaction that required you to ascertain the identity of your client, the business relationship with that client ceases in the case of non-account-based business relationships. In the case of clients who hold an account, the business relationship ceases five years after the client closes that account.

Once the business relationship is established, you must also:

- conduct ongoing monitoring of your business relationship with your client; and
- keep a record of the measures you take to monitor your business relationship and the information you obtain as a result. See section 5.1 for a description of what information you must keep for this record.

Ongoing monitoring

Ongoing monitoring means that you have to monitor your business relationship with a client on a periodic basis. Use your risk assessment of the client with whom you have a business relationship to determine how frequently you will monitor that business relationship. The risk assessment requires you to consider each one of your 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 you can demonstrate that you put your client in the correct risk category, according to your policies and procedures, and risk assessment. You have to perform ongoing monitoring of each business relationship in order 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 activities; and
- determine whether the transactions or activities are consistent with the information previously obtained about the client, including the risk assessment of the client.

The above-listed requirements do not need to follow the same timeframe, so long as you monitor your high-risk clients more frequently and with more scrutiny than you do your low-risk clients.

In order to keep client and beneficial ownership information up to date, you may ask clients with account-based business relationships to confirm the information you have on record periodically throughout your regular interactions with them. For clients in non-account-based business relationships, you may update the

information you have on record every time the client conducts a transaction that requires you to ascertain their identity.

As an example, you may choose to reassess the level of risk associated with a client's transactions and activities, and to determine whether the transactions or activities are consistent with the information you have on your client, for your low-risk clientele, every two years, while performing the same monitoring of your high-risk clients on a more frequent basis. However, depending on the circumstances of your operations, a different ongoing monitoring period for low-risk clients may be appropriate.

In the context of monitoring on a periodic basis, your monitoring will vary depending on your risk assessment of your client. As part of your ongoing monitoring obligations, you must monitor all of your business relationships, and you must monitor business relationships you consider high-risk more frequently, as well as update client identification information and adopt any other appropriate enhanced measures.

Here is a non-exhaustive list of enhanced measures you could take to mitigate the risk in cases of high-risk business relationships:

- Obtaining additional information on the client (e.g. occupation, volume of 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.
- Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar client due diligence standards.
- 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.

If as a result of your ongoing monitoring you consider that the risk of a money laundering or a terrorist financing offence in a business relationship is high, your risk assessment in your compliance regime must treat that client as a high risk. In this case, you must conduct more frequent monitoring of your business relationship with that client, update that client's identification information more

frequently, and adopt any other appropriate enhanced measures (see examples above).

Exception

The requirement to conduct ongoing monitoring does not apply to a group plan account held within a dividend or a distribution reinvestment plan if the sponsor of the plan is an entity that trades shares or units on a Canadian stock exchange and operates in a country that is a member of the Financial Action Task Force.

Guideline 4: Implementation of a Compliance Regime provides more information about risk assessment requirements.

5.1 Business relationship record

When you enter into a business relationship with a client, you have to keep a record of the purpose and intended nature of the business relationship. You also have to review this information on a periodic basis and keep it up to date. This is done to ensure that you continue to understand your client's activities over time so that any changes can be used to assess or detect high-risk transactions and activities. This may lead you to increase the frequency of ongoing monitoring, update their client identification information more frequently, and adopt any other appropriate enhanced measures (see examples above).

The purpose and intended nature of the business relationship is information that should allow you to anticipate the transactions and activities of your client.

For clients who already hold accounts, you may use the information found in the intended use of the account record, in a client credit file, in a credit card account record or in an ongoing service agreement, as the purpose and intended nature of the business relationship with that client. You do not need to create a new record if you are able to retrieve this information from the records you currently hold. You must obtain this information at the opening of a new account.

For clients who do not hold an account but with whom you have a business relationship on the basis that they have completed two transactions that required you to ascertain their identity, or in the case of entities, to confirm their existence; you must document the purpose and intended nature of the business relationship that best describes your dealings with that client.

Here is a short, non-exhaustive list of examples of purpose and intended nature of a business relationship in your sector:

Personal banking:

- to manage household expenses and bills
- to receive directly deposited employment or pension income
- to save for retirement

Commercial banking:

- to deposit daily receipts for a business
- to make payments to employees (payroll)
- to make payments to suppliers

6 Records about Beneficial Ownership and Control

You have to confirm the existence of a corporation or other entity at the opening of an account. At the same time, you have to obtain, take reasonable measures to confirm, and keep records of the information about the entity's beneficial ownership. Beneficial ownership refers to the identity of the individuals who ultimately control the corporation or entity, and cannot be another corporation or another entity. You must search through as many levels of information as necessary in order to determine beneficial ownership. However, there may be cases where there is no individual who owns or controls 25% or more of an entity. You must still keep a record of the measures you took and the information you obtained in order to reach that conclusion..

In this context, reasonable measures to confirm the accuracy of beneficial ownership information would include asking the client to provide documentation. You can rely on the information provided by clients, but you should use discernment when determining if the documentation is appropriate. Documents and references that you obtain to confirm the information (such as the website where you found the information) have to be kept in your records.

Here is a short, non-exhaustive list of documents that could be provided by clients to confirm beneficial ownership information:

In the case of corporations:

- Articles of incorporation
- Annual returns
- Shareholder agreements

In the case of entities other than corporations:

- Articles of constitution
- Partnership agreements
- Records of decisions

You have to obtain, take reasonable measures to confirm, and keep a record of the following beneficial ownership information:

- If the entity is a corporation:
 - the names of all directors of the corporation;
 - the names and addresses of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation; and

- information on the ownership, control and structure of the corporation.

The following is an example of ownership, control and structure of a corporation:

ABC Canada Inc. is a for-profit corporation with 100 privately traded shares in circulation. It is incorporated pursuant to the Canada Business Corporations Act. John Brown owns 15 of the shares and Green Company Ltd. owns the remaining 85 shares. James Smith is President of ABC's board of directors; his wife, Jane Smith, is ABC's Chief Financial Officer; and their three children make up the other members of the board.

In this example:

- *Ownership of the corporation is shared by John Brown (15 % of the shares) and Green Company Ltd. (85% of the shares);*
- *All members of the board of directors (the 5 members of the Smith family) exercise control of the corporation. Because Green Company Ltd. owns 85% of the corporation's shares, it also exercises control. However, in a case like this, you must research further into the ownership until you find an individual who owns enough shares in Green Company to own or control 25% or more of ABC Canada or until you find that there is no such individual;*
- *The structure of the corporation is that of a privately traded, for-profit corporation incorporated pursuant to the Canada Business Corporations Act.*
- If the entity is a trust:
 - the names and addresses of all trustees and all known beneficiaries and settlors of the trust; and
 - information on the control and structure of the trust.

The trust deed will provide you the information on the control and structure of the trust. If you are unable to obtain the names and addresses of the trustees, beneficiaries or settlors of the trust, you must find the name of the senior managing officer of the trust, that is, the person in the trust company who is in fact responsible for the management of that trust, such as an account manager.

- If the entity is other than a corporation or trust:
 - the names and addresses of all individuals who directly or indirectly own or control 25% or more of the entity; and
 - information on the ownership, control and structure of the entity.

The following is an example of ownership, control and structure of an entity that is neither a corporation nor a trust:

Rainbow Money Services is a money services business (MSB) in Vancouver owned by Howard and Betty. Howard and Betty paid a lawyer to draft a partnership agreement for the business, which they both signed. According to the agreement, Howard will invest \$100,000 in the partnership to buy equipment and rent space for the MSB, and Betty will be solely responsible for operating the MSB and performing its business. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. Howard and Betty will split the income from the MSB 50/50, and if they decide to end the partnership, Howard will get 85% of the proceeds of the sale of the business assets, while Betty will get 15%.

In this example:

- *Ownership of the entity is shared between Howard and Betty;*
- *Howard and Betty both control the partnership;*
- *The structure of the entity is a partnership between Howard and Betty, constituted pursuant to a contract governed by the laws of British Columbia.*

If this information cannot be obtained or its accuracy cannot be confirmed, you 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 your risk assessment document of your compliance regime and undertake more frequent monitoring, updating of client identification information, and any other appropriate enhanced measures (see examples in section 5).

You 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, the senior managing officer of a corporation or 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.

In the context of this section, the senior managing officer of a trust is the trustee, that is, the person who is authorized to administer or execute on that trust.

To ascertain the identity of the most senior managing officer, use one of the methods described in section 4.12 or obtain it through public sources. You also have to keep a record of this information.

The requirement to confirm the existence of a corporation, trust or other entity at the opening of an account does not apply to a group plan account held within a dividend or a distribution reinvestment plan if the sponsor of the plan is an entity that trades shares or units on a Canadian stock exchange and operates in a country that is a member of the Financial Action Task Force.

Not-for-profit organization

If you have to confirm the existence of an entity that is a not-for-profit organization, you 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, you 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, you can ask the client.

Credit card acquiring businesses

If you are carrying on activities as a credit card acquiring business, beneficial ownership requirements do not apply to those activities. For more about credit card acquiring businesses, see the information in subsection 3.1.

Keeping beneficial ownership information up to date

According to your compliance regime's assessment of risk, in all situations, you have to keep beneficial ownership information up to date. Measures to keep beneficial ownership information up to date include those explained at the beginning of section 6 that are applicable at account opening.

The frequency with which beneficial ownership information is to be kept up to date will vary depending on your risk assessment of your client. As part of your ongoing monitoring obligations, you have to keep all beneficial ownership information up to date. For high-risk clients, you must update beneficial ownership information more frequently and perform more frequent monitoring, as well as adopt any other appropriate enhanced monitoring measures (see examples in section 5).

Guideline 4: Implementation of a Compliance Regime provides more information about risk assessment requirements.

7 Third Party Determination and Related Records

If you open an account for a client that is a credit card acquiring business, for use in relation to that business, you do not have to make a third party determination about that client.

If, on the other hand, you are yourself carrying on activities as a credit card acquiring business, the requirements for third party determination and related records do not apply to those activities.

7.1 Third party determination

You have to make a third party determination when you have to keep any of the following records.

- **Large cash transaction record**
Whenever you have to keep a large cash transaction record (as described in subsection 3.2), you have to take reasonable measures to determine whether the individual who gives you the cash is acting on the instructions of a third party.

In this context, a third party is an individual or entity other than the individual who conducts the transaction.

- **Signature card or an account operating agreement (when opening accounts)**
Whenever you open an account and are required to keep a signature card or an account operating agreement as explained in subsections 3.3 and 3.5, you have to take reasonable measures to determine whether the account is to be used by or on behalf of a third party.

In this context, a third party is an individual or entity, other than the account holder or those authorized to give instructions about the account, who directs what happens with the account. For example, if an account were opened in one individual's name for deposits that are directed by someone else, the other person or entity would be a third party. As another example, parents who decide to open an education savings account for their child would not be acting on the instructions of the child and therefore would not be acting on behalf of a third party.

You do **not** have to make any third party determination about an **account** if the account holder is another financial entity or a securities dealer engaged in dealing in securities in Canada.

This third party determination does not apply to credit card accounts, as you do not have to keep a signature card or an account operating agreement for them.

When you are 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 you is acting on someone else’s instructions. If so, that someone else is the third party.

In making a third party determination when employees are acting on behalf of their employers, they are considered to be acting on behalf of a third party. The only exception to this is when an employee deposits cash to the employer’s account. In that case, the employee is not considered to be acting on behalf of a third party. This is only true if the account in which the employee deposits cash is a **business** account.

Reasonable measures

What constitutes reasonable measures in making a third party determination will vary in accordance with the context in which they occur, and therefore could differ from one situation to the next. However, reasonable measures would include retrieving the information already contained in your files or elsewhere within your business environment, or obtaining the information directly from the client.

7.2 Third party records

If you determine that there is in fact a third party as explained above, you have to keep a record of the following information:

- the third party’s name, address and principal business or occupation;
- if the third party is an individual, the third party’s date of birth;
- the incorporation number and place of incorporation if the third party is a corporation; and
- in the case of a large cash transaction, the nature of the relationship between the third party and the individual who gives you the cash; or
- in the case of an account, the nature of the relationship between the third party and the account holder. For examples of third party relationships, see field 18 of Part G in the large cash transaction report.

For more information about recording business or occupation, see subsection 3.2, under the heading “Contents of a large cash transaction record.”

If you are not able to determine that there is in fact a third party, but you have reasonable grounds to suspect that there are instructions of a third party involved, you have to keep a record to indicate the following:

- in the case of a large cash transaction, whether, according to the individual giving the cash, the transaction is being conducted on behalf of a third party; or
- in the case of an account, whether, according to the individual authorized to act for the account, the account will be used by or on behalf of a third party.

This record must also indicate details of why you suspect the individual is acting on a third party's instructions.

You do **not** have to keep the third party record described above for an **account** if the following conditions are met:

- the account is opened by a legal counsel, an accountant or a real estate broker or sales representative; and
- you have reasonable grounds to believe that the account is to be used only for their clients.

If an account is for or on behalf of future and unknown clients, employees, etc., of the individual or entity opening the account, you should keep a record indicating that the account is to be used by or for third parties who are not known at the time of account opening.

Trust company

If you are a trust company, you have to keep a record concerning a trust, as explained in subsection 3.10. If you have to keep such a record for a personal trust (other than a trust created by a will), you also have to keep a record about each of the beneficiaries that are known to you at the time you become a trustee for the trust. The information required in this record is the name, address and principal business and occupation of each beneficiary known at that time. If the beneficiary is an individual, the record also has to include the beneficiary's date of birth.

8 Politically Exposed Foreign Person Determination and Related Records

A politically exposed foreign person is an individual who holds or has ever held one of the following offices or positions in or on behalf of 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 foreign 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).

An individual or family member described above is a politically exposed foreign person regardless of their citizenship, residence status or birth place.

Exceptions

The requirements described in this section do not apply in the exceptions described under the heading "Certain types of accounts or transactions" in subsection 4.2.

Furthermore, if you are carrying on activities as a credit card acquiring business, the requirements for politically exposed foreign person determination and related records do not apply to those activities. For more about credit card acquiring businesses, see subsection 3.1.

8.1 Politically exposed foreign person determination

You have to take reasonable measures to determine whether you are dealing with a politically exposed foreign person for new or existing accounts or for certain electronic funds transfers.

Once you have determined that an individual is a politically exposed foreign person, you will not have to do it again. However, if you initially determined that an individual was not a politically exposed foreign person, you must still take reasonable measures to determine whether you are dealing with a politically exposed foreign person for every subsequent account opening or for prescribed electronic funds transfers, since the client's status may have changed.

New accounts

When you open an account for an individual, including a credit card account, you have to take reasonable measures to determine whether you are dealing with a politically exposed foreign person. This has to be done within 14 days after the new account is activated.

If you determine that an individual is a politically exposed foreign person for a new account, you also have to do the following:

- get senior management's approval to keep the account open within 14 days after the new account is activated;
- take reasonable measures to establish the source of funds that have been, will be or are expected to be deposited in that account. Once you have determined the source of funds for the account, you are not required to do so again for future deposits, unless ongoing monitoring triggers the need to do so; and
- perform enhanced ongoing monitoring of activities for that account to detect suspicious transactions.

You have to make the determination and get senior management approval within a single period of 14 days. For example, if it takes you 5 days after the new account is activated to make the determination that you are in fact dealing with a politically exposed foreign person, you have 9 days left to get senior management approval to keep the account open.

Existing accounts

For existing account holders, including credit card accounts, you also have to take reasonable measures to determine whether you are dealing with a politically exposed foreign person. This is to be done based on your compliance regime's risk assessment regarding situations considered to be higher-risk for money laundering or terrorist financing. *Guideline 4: Implementation of a Compliance Regime* provides more information about risk assessment requirements.

If you determine that an individual is a politically exposed foreign person for an existing account, you also have to do the following:

- get senior management's approval to keep the account open within 14 days after you determined that the existing account holder is a politically exposed foreign person;
- take reasonable measures to establish the source of funds that have been, will be or are expected to be deposited in that account. Once you have determined the source of funds for the account, you are not required to do so again for future deposits, unless ongoing monitoring triggers the need to do so; and
- perform enhanced ongoing monitoring of activities for that account to detect suspicious transactions.

Electronic funds transfers

An electronic funds transfer (EFT) means the transmission—through any electronic, magnetic or optical device, telephone instrument or computer—of instructions for the transfer of funds to or from Canada. In the case of messages sent through the SWIFT network, only SWIFT MT 103 messages are included. An EFT does not include the instructions for the transfer of funds from one place in Canada to another in Canada.

You have to take reasonable measures to determine if the **initiator** of an outgoing EFT of \$100,000 or more is a politically exposed foreign person. The initiator means the individual who requested the EFT whether the individual is acting on behalf of an entity (including a corporation) or on their own behalf. This determination has to be done within 14 days after the transaction occurred.

For the purposes of politically exposed foreign person determination, an outgoing EFT means the transmission of instructions for the transfer of \$100,000 or more outside Canada at the request of a client.

If an individual who is the initiator of an EFT of \$100,000 or more is a politically exposed foreign person, you will also have to do the following:

- take reasonable measures to establish the source of funds used by the initiator for the transaction; and
- within 14 days after the transaction occurred, get a member of senior management to review the transaction.

When an individual is the **beneficiary** of an incoming EFT of \$100,000 or more, you have to take reasonable measures to determine whether you are dealing with a politically exposed foreign person. This has to be done within 14 days after the transaction occurred. In this particular case, the beneficiary is the individual who is the recipient of the funds of \$100,000 or more from outside Canada. For the purposes of politically exposed foreign person determination, an incoming EFT means the reception of instructions for the transfer of \$100,000 or more from outside Canada, at the request of a client.

If an individual who is the beneficiary of an EFT of \$100,000 or more is a politically exposed foreign person, you also have to get a member of senior management to review the transaction, within 14 days after the transaction occurred.

You have to make the determination and get senior management to review the transaction within a single period of 14 days. For example, if it takes you 5 days after the transaction to make the determination that you are in fact dealing with a politically exposed foreign person, you have 9 days left to get senior management to review the transaction.

Reasonable measures

In the context of this subsection, reasonable measures to determine whether or not you are dealing with a politically exposed foreign person include the following:

- asking the client; or
- consulting a credible source of commercially or publicly available information about politically exposed persons.

In establishing the source of funds, reasonable measures also include asking the client.

Senior management

Also in the context of this section, senior management means an individual who has the following:

- authority to make and be held accountable for management decisions about this type of account or transaction;
- awareness of the money laundering or terrorist financing risks to which the financial entity or this type of account or transaction is exposed; and
- awareness of politically exposed foreign persons.

8.2 Politically exposed foreign person records

Once an account has been approved or a transaction reviewed, as explained in subsection 8.1, you have to keep a record of the following:

- the office or position of the individual who is a politically exposed foreign person;
- the source of the funds, if known, that are or are expected to be deposited in the account or used for the transaction;
- the date you determined the individual to be a politically exposed foreign person;
- the name of the member of senior management who approved the account to be kept open or reviewed the transaction; and
- the date the account was approved to be kept open or the date the transaction was reviewed.

9 Correspondent Banking Relationships and Related Records

9.1 What is a correspondent banking relationship?

A correspondent banking relationship is one created by an agreement or arrangement between a **foreign** financial institution and a bank, a credit union, a caisse populaire or a trust company. It only applies to an agreement where the bank, credit union, caisse populaire or trust company is to provide services, such as (but not limited to) international electronic funds transfers, cash management and cheque clearing, to the foreign financial institution. If the agreement were only for the foreign financial institution to provide services to the bank, credit union, caisse populaire or trust company, then it would **not** be considered a correspondent banking relationship for these purposes.

In this context, a correspondent banking relationship includes only an arrangement (as described above) that you, as a bank, credit union, caisse populaire, financial services cooperative, credit union central, or trust company, have directly with a foreign financial institution. It does not include access to your

services through an arrangement that the foreign financial institution has with another financial entity or with an association of yours, such as your credit union central.

Credit card acquiring businesses

If you are carrying on activities as a credit card acquiring business, requirements related to correspondent banking relationships do not apply to those activities.

9.2 Before you enter into a correspondent banking relationship

Before you establish a correspondent banking relationship, you have to determine that the foreign financial institution is not a shell bank. If you determine that it is, you cannot enter into a correspondent banking relationship with that entity.

A shell bank is a foreign financial institution that does not have a physical presence in any country, unless that institution is controlled by or under common control with a depository institution, credit union or another foreign financial institution that maintains a physical presence either in Canada or in a foreign country. In this context, physical presence means that an institution maintains a place of business as follows:

- located at a fixed address in a country where the institution is authorized to conduct its banking activities;
- which can be inspected by the banking authority that licensed the institution for banking activities; and
- where the institution maintains its operating records and employs at least one full-time employee.

Before you enter into a correspondent banking relationship, you also have to get senior management approval and set out in writing both your and the foreign financial institution's obligations for the correspondent banking services. In this context, senior management means an individual who has the following:

- overall responsibility for the activities regarding the line of business related to the correspondent banking relationship;
- authority to make and be held accountable for management decisions about that line of business;
- awareness of the money laundering or terrorist financing risks to which the financial entity or the line of business is exposed; and
- awareness of banking relationships and the responsibility for oversight of those relationships.

9.3 Correspondent relationship records

If you enter into a correspondent banking relationship, you have to keep a record about the foreign financial institution with the following information and documents:

- its name, address and primary business;
- the names of its directors;
- a copy of its most recent annual report or audited financial statement;
- a copy of one of the following legal documents:
 - the foreign financial institution's banking licence, banking charter, authorization or certification to operate from the relevant regulatory agency;
 - its certificate of corporate status; or
 - other similar document;
- a copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity;
- the anticipated correspondent banking account activity of the foreign financial institution, including the products or services to be used; and
- the measures you took to find out whether there are any civil or criminal sanctions imposed against the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements, and the results of those measures (see subsection 9.4 for more information about the required measures).

Statements

You will also have to keep the following:

- a statement from the foreign financial institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks; and
- a statement from the foreign financial institution that it is compliant with anti-money laundering and anti-terrorist financing legislation in its own jurisdiction.

Record keeping obligations at the opening of account

Record keeping obligations that would normally apply for the opening of accounts will not apply for accounts that are opened for the foreign financial institution as a result of the correspondent banking relationship.

9.4 Confirming identification and other information

When you enter into a correspondent banking relationship, you also have to do the following:

- Confirm the name and address of the foreign financial institution by examining a copy of its banking licence, banking charter, authorization or certification to operate from the relevant regulatory agency or a certificate of corporate status or another similar document.

- Take reasonable measures to find out whether the foreign financial institution has anti-money laundering and anti-terrorist financing policies and procedures in place, including procedures for the approval of opening new accounts. In this context, reasonable measures include asking the foreign financial institution for the information about their policies and procedures. If they do not have such policies and procedures in place, you have to take reasonable measures to conduct ongoing monitoring of all transactions within the correspondent banking relationship to detect suspicious transactions.
- Take reasonable measures to find out, based on publicly available information, whether there are any civil or criminal sanctions imposed against the foreign financial institution in respect of anti-money laundering or anti-terrorist financing requirements. If so, take reasonable measures to conduct ongoing monitoring of all transactions within the correspondent banking relationship to detect suspicious transactions.

Reasonable measures to conduct ongoing monitoring will vary in accordance with the context in which transactions occur, and therefore could differ from one situation to the next. If a suspicious transaction is detected, you must submit a suspicious transaction report to FINTRAC. For more information about suspicious transactions and how to report them, see *Guideline 2: Suspicious Transactions* and *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC*.

If customers of the foreign financial institution will have direct access to the services provided under the correspondent banking relationship, you will have to take reasonable measures to do the following:

- Find out whether the foreign financial institution has ascertained identification for customers that have direct access to your accounts, in a way that is consistent with your identification obligations for signature cards, money orders, traveller's cheques or other similar negotiable instruments, foreign currency exchanges or electronic funds transfers; and
- Establish whether the foreign financial institution has agreed to provide you with relevant customer identification information upon request.

In this context, reasonable measures to find out include asking the foreign financial institution.

10 Foreign Subsidiaries or Branches

If you are a financial entity, that has foreign branches or foreign subsidiaries which carry out activities similar to those of a financial entity, securities dealer or insurance broker; and that are wholly owned by you or have consolidated financial statements with you, you have the following requirements:

- Develop policies to establish requirements with respect to record keeping and their retention, and ascertain client identity.
- Establish and implement a compliance program which must also include the risk assessment of money laundering or a terrorist activity financing offence, and risk mitigation controls when the risk is considered to be high. These requirements must be similar to those in Canada.

If you have a Board of Directors, they shall approve these policies.

You must ensure that your foreign branches or foreign subsidiaries apply these policies to the extent it is permitted by the laws of the country in which the foreign subsidiary or foreign branch is located. If they cannot implement these policies or part of them because they conflict with the laws of the country in which they are located, you must keep a record including the reasons why these policies cannot be implemented and provide a copy, within a reasonable time period, to your regulating body and FINTRAC.

Exceptions to definition of Foreign Subsidiaries

These requirements do not apply to you if you are an authorized foreign bank within the meaning of section 2 of the *Bank Act* or an agent of the crown that accepts deposit liabilities.

These requirements do not apply to subsidiaries of foreign subsidiaries. For example, if Canadian Bank A has a foreign subsidiary (Subsidiary A) and there is a Subsidiary B of Subsidiary A, then these requirements do not apply to Subsidiary B.

These requirements do not apply to you if you are the Canadian subsidiary of a foreign entity, when the foreign entity has developed policies that are similar to Canada's compliance regime requirements (see section 3 of this guideline) and also have in place policies to assess the risk of money laundering and terrorist activity financing. For example, when Foreign Bank A with subsidiaries A and B in Canada already has policies regarding client identification, record keeping and the establishment of a compliance regime, then these requirements do not apply to the Canadian subsidiaries A and B.

For more information about the compliance regime requirements, refer to Section 3 of *Guideline 4: Implementation of a Compliance Regime*. The Canadian record keeping and client identification requirements are explained in this guideline, with the following exceptions:

- Requirements concerning politically exposed foreign person determination and related records (see section 8) do not apply to the foreign subsidiary or branch.

- Requirements concerning correspondent banking (see section 9) do not apply to the foreign subsidiary or branch.
- Requirements concerning information to be included with outgoing or incoming electronic funds transfers (see subsection 3.9 under the headings “Information to include with outgoing transfers” and “Information to be included with incoming transfers”) do not apply to the foreign subsidiary or branch.

Information Exchange between Domestic and Foreign Affiliated Entities

If you are a financial entity is affiliated with another entity or a foreign entity that carries out activities similar to those of a financial entity, securities dealer or insurance company, you must develop and apply policies and procedures in relation to the exchange of information between you and your affiliated entities. The purpose of this exchange of information is to help detect and deter money laundering and the financing of terrorist activities and to assist your risk assessment of such an offence.

As part of your risk assessment, you may want to keep a record including the rationale as to why these policies cannot be implemented by the affiliated entities.

Affiliated entity means if one of you is wholly owned by the other, if both of you are wholly owned by the same entity or if your financial statements are consolidated

11 How Should Records Be Kept?

You should maintain an effective record keeping system to enable FINTRAC to have access to the records in a timely fashion. Your records have to be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them.

For the requirements explained in this guideline, you can keep records in a machine-readable or electronic form, as long as you can readily produce a paper copy from it. For example, if you have a document imaging system, you do not have to produce the original document for these purposes, as long as you can print the imaged one.

The record keeping requirements explained in this guideline are about each record to be kept. Your record keeping system can store the information required for any one record separately, as long as you are able to readily retrieve and put the information together for the record whenever necessary.

Also, if you keep records electronically that require a signature on them, such as a signature card or a cleared cheque for example, an electronic signature of the individual who signed the record has to be retained. An electronic signature means an electronic image of the signature and does not include a personal identification number (PIN).

You are not required to keep a copy of the reports you make to FINTRAC (other than the suspicious transaction report as explained in subsection 3.11), but you may choose to do so. It is recommended that you keep the information that FINTRAC sends you in the acknowledgement message about each report processed. This provides the date and time the report was received along with its identification number.

Timeframe for keeping records

In the case of signature cards, account operating agreements, client credit files, credit card applications, records setting out the intended use of the account, politically exposed foreign person records regarding an account, or a credit card account, these records have to be kept for five years from the day of closing of the account to which they relate.

In the case of records to confirm the existence of an entity (including a corporation), beneficial ownership records, politically exposed foreign person records regarding transactions and records about a corresponding banking relationship, they have to be kept for five years from the day the last business transaction was conducted.

In the case of a copy of a suspicious transaction report, the record has to be kept for a period of at least five years following the date the report was made.

In the case of all other records, the records must be kept for a period of at least five years following the date they were created.

Employees or contractors who keep records for you

Your employees who keep records (as described in section 3) for you are not required to keep those records after the end of their employment with you. The same is true for individuals in a contractual relationship with you, after the end of that contractual relationship. This means that you have to get and keep the records that were kept for you by any employee or contractor before the end of that individual's employment or contract with you.

12 Penalties for Non-Compliance

Failure to comply with your record keeping or client identification requirements can lead to criminal charges against you. Conviction of failure to retain records could lead to up to five years imprisonment, to a fine of \$500,000, or both. Alternatively, failure to keep records or ascertain the identity of clients can lead to

an administrative monetary penalty. For more information on penalties, you can also consult the “Penalties for non-compliance” section of FINTRAC's website.

13 Comments?

These guidelines will be reviewed on a periodic basis. If you have any comments or suggestions to help improve them, please send your comments to the mailing address provided below, or by email to guidelines-lignesdirectrices@fintrac-canafe.gc.ca.

14 How to Contact FINTRAC

For further information on FINTRAC and its activities, reporting and other obligations, please go to FINTRAC's website (<http://www.fintrac-canafe.gc.ca>) or contact FINTRAC:

Financial Transactions and Reports Analysis Centre of Canada
234 Laurier Avenue West, 24th floor
Ottawa ON K1P 1H7
Canada

Toll-free: 1-866-346-8722