



Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada

Guideline 6I: Record Keeping and Client Identification for Dealers in Precious Metals and Stones

Guideline 6I: Record Keeping and Client Identification for Dealers in Precious Metals and Stones

: YVfi Ufm&\$%

This replaces the previous version of *Guideline 6I: Record Keeping and Client Identification for Dealers in Precious Metals and Stones* issued in July 2010. This version includes guidance on obligations, which come into effect February 1, 2014, to better understand your clients and related business relationships.

Table of Contents

1	General	3
2	Record Keeping and Client Identification Obligations	5
3	Records to be Kept	8
3.1	General exceptions to record keeping	8
3.2	Large cash transaction records	8
3.3	Suspicious transaction report records	10
3.4	Identification information on all records	10
4	Client Identity	11
4.1	When and how do you have to ascertain client identity?	11
4.2	General exceptions to client identification.....	11
4.3	Client identity for large cash transactions	12
4.4	Client identity for suspicious transactions	12
4.5	How to ascertain the identity of an individual.....	12
4.6	Keeping client identification information up to date.....	16
5	Business Relationship and Related Records	16
5.1	Business relationship record.....	18
6	Third Party Determination and Related Records	19
6.1	Third party determination.....	19
6.2	Third party records	19
7	How Should Records be Kept?	20
8	Penalties for Non-Compliance	21
9	Comments?	21
10	How to Contact FINTRAC	21

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 dealers in precious metals and stones.

If you are a dealer in precious metals and stones, you are subject to the record keeping and client identification requirements explained in this guideline if you engage in the activities described in section 2.

This guideline has been prepared to help you meet your record keeping and client identification obligations. 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 (financial entities; securities dealers; life insurance companies, brokers and agents; money services businesses; agents of the Crown that sell or redeem money orders; real estate; casinos; British Columbia notaries and accountants).

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 persons and 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 credit cards, debit cards, cheques, money orders, or other similar negotiable instruments.

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, retention period for your records may vary for purposes other than what is described in this guideline.

2 Record Keeping and Client Identification Obligations

A dealer in precious metals and stones means an individual or an entity that buys or sells precious metals, precious stones or jewellery, in the course of its business activities. Precious metals mean gold, silver, palladium or platinum whether in coins, bars, ingots, granules or in any other similar form. Precious stones mean diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. Jewellery means objects made of precious metals, precious stones or pearls intended for personal adornment, such as earrings, bracelets, rings, necklaces, brooches, watches, etc.

When is a dealer in precious metals and stones subject to the obligations?

As a dealer in precious metals and stones, you are subject to the obligations explained in this guideline if you ever engage in the purchase or sale of precious metals, precious stones or jewellery in an amount of \$10,000 or more in a single transaction. In other words, you are not subject to these requirements if you engage only in purchases or sales of less than \$10,000 per transaction. Once you engage in such a transaction of \$10,000 or more, whether it is a purchase for inventory, a sale to a client or another type of transaction, the requirements explained in this guideline apply to you from the day of that purchase, sale or transaction and for the future.

If you are an agent of the Crown (that is, a government department or an agent of her Majesty in right of Canada or of a province), you are considered to be a dealer in precious metals and stones if you sell precious metals to the public in an amount of \$10,000 or more in a single transaction.

Examples of those subject to these obligations

The following are examples of those who are subject to the obligations:

- A retailer or wholesaler that sells or buys precious metals, precious stones or jewellery for an amount of \$10,000 or more in a single transaction. The obligations apply to that retail or wholesale business as these transactions are not considered manufacturing jewellery.
- A manufacturer that sells jewellery to a consumer in an amount of \$10,000 or more in a single transaction, even if just once. In this case, the manufacturer would be subject to the obligations for all of its activities from the time of that sale and onwards.

Exclusions

As a dealer in precious metals and stones, a single transaction of \$10,000 or more to purchase or sell precious metals, precious stones or jewellery will **not** make you subject to the obligations if that transaction is carried out for, in connection with, or for the purpose of:

- manufacturing jewellery;
- extracting precious metals or precious stones from a mine; or
- cutting or polishing precious stones.

If you conduct manufacturing, mining, cutting or polishing and all or substantially all of your purchases and sales are related to these activities, you are **not** subject to these obligations **unless** you conduct a transaction of \$10,000 or more with a consumer. In this context, “all or substantially all” means that 90% or more of your purchases or sales are related to manufacturing, mining, cutting or polishing activities. In determining whether these exclusions apply to you, consider the following three questions:

- Are less than 90% of your annual sales related to manufacturing, mining, cutting or polishing activities?
- Are less than 90% of your annual purchases related to manufacturing, mining, cutting or polishing activities?
- Did you sell to a consumer precious metals, precious stones or jewellery in an amount of \$10,000 or more in a single transaction?

If you answer *no* to all of the above-noted questions, you are **not** subject to the obligations. If you answer *yes* to one of these questions, and you have made a purchase or sale of precious metals, precious stones or jewellery of \$10,000 or more, you are subject to the obligations.

Meaning of manufacturing jewellery

In this context, manufacturing jewellery includes the following activities:

- the moulding of precious metals to obtain jewellery;
- the assembling of precious metals, precious stones or pearls to obtain jewellery;
- the blending and mixing of precious metals and alloys to obtain gold, silver, platinum and palladium;
- the applying of coatings (such as gold or silver) or finishes to or on jewellery; and
- other similar activities.

In addition, manufacturing jewellery excludes the following:

- the sole packaging or repackaging of jewellery;
- the repair of jewellery;
- the sizing or resizing of jewellery;
- the sole engraving, chasing, or etching of jewellery.

Examples of those not subject to these obligations

The following are examples of those who are **not** subject to the obligations:

- A manufacturer that sells at the retail level precious metals, precious stones or jewellery, but only in amounts under \$10,000 per transaction.
- A retailer that sells jewellery solely made of materials other than precious metals or precious stones (for example, stainless steel, crystal, Murano glass, copper, etc.).

- A manufacturer that only sells to or purchases from manufacturers, wholesalers or retailers.

As a dealer in precious metals and stones, your record keeping and client identification obligations are as follows:

- When you conduct a large cash transaction, your record keeping and client identification obligations are as follows:
 - Keep a large cash transaction record (see section 3);
 - Ascertain the identity of the individual (see section 4); and
 - Make a third party determination and keep related records (see section 6).
- 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, identify 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, you may have a business relationship with that client. If so, your obligations are as follows:
 - Keep a record of the purpose and intended nature of the business relationship (see section 5).
 - Conduct enhanced monitoring of **high-risk** business relationships and keep related records (see section 5).

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. For the federal Agents of the Crown, the use of personal information in Canadian commercial activities is protected by the *Privacy Act*. 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 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 dealer in precious metals and stones, you have to keep the following records in addition to the records described in sections 5 and 6 if you are subject to the obligations as explained in section 2:

- Large cash transaction records;
- Suspicious transaction report records.

Details about each of these types of records are provided in subsections 3.2 and 3.3. Also, section 7 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.

3.2 Large cash transaction records

This is a record you have to keep 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 brings you \$10,000 in cash to purchase precious metals, you have to keep a large cash transaction record. If you sell precious metals, precious stones or jewellery left on consignment with you, for which you receive an amount of \$10,000 or more in cash, you also have to keep a large cash transaction record for them. 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. For example, a client wants to buy jewellery and gives a lay away deposit of \$5,000 in cash. The client comes back within 24 consecutive hours and pays the difference of \$8,000 in cash. 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 you are an auctioneer that has precious metals, precious

stones or jewellery left with you for an auction sale. The same exceptions apply if the cash is received from a financial entity or a public body.

In this context, a financial entity means any of the following:

- a bank (that is, one that is listed in Schedule I or II of the *Bank Act*) or an authorized foreign bank with respect to its operations in Canada;
- a credit union or a caisse populaire;
- a financial services cooperative (in the province of Quebec) or a credit union central (in all other provinces);
- a trust and loan company; or
- an agent of the Crown that accepts deposit liabilities.

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.

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 name, date of birth and address of the individual from whom you received the cash and that individual's principal business or occupation;
- the date of the transaction;
- the purpose, details and type of transaction (for example, the cash was to purchase precious metals, precious stones or jewellery, 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.
- where the amount is received for the sale of precious metals, precious stones or jewellery:
 - the type of precious metals, precious stones or jewellery involved in the transaction;
 - the value of the transaction, if different from the amount of the cash received; and

- the wholesale value of the transaction (that is, the amount you had paid for the item sold).

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.” For more examples, consult the resource on occupational information in Canada, called the National Occupational Classification (NOC). This information is available from the A-Z Index on the Human Resources and Skills Development Canada website (<http://www.hrsdc.gc.ca>).

If you have to ascertain the identity of the individual conducting the large cash transaction, see subsection 3.4 for additional information that is required on the large cash transaction record.

3.3 Suspicious transaction report records

When you have to report a suspicious transaction to FINTRAC, you have to keep a copy of the report. There is no threshold (that is, no dollar amount) for a suspicious transaction. See *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* for more information about obligations related to this report.

3.4 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 ascertain 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 4.5), 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 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 identify the individual;
- 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; and
- If you use an attestation signed by a commissioner of oaths in Canada or a guarantor in Canada, you have to keep the attestation.

4 Client Identity

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

As a dealer in precious metals and stones, you have client identification obligations when you engage in the activities described in section 2. You have to take the following measures to ascertain the identity of individuals, subject to the general exceptions in subsection 4.2.

If you suspect that the transaction is related to a money laundering or terrorist financing offence, you must file a suspicious transaction report. See section 4.4 for more information.

Subsections 4.3 and 4.4 explain the need to ascertain the identity of individuals when an event triggers the requirement. In these events, you must ascertain the identity of an individual, unless an exception applies as explained below.

See 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 confirm 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 identify that individual again.

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—that is, the individual who has physically given you the cash—at the time of the transaction, if you have to keep a large cash transaction record for it, as described in subsection 3.2.

See subsection 4.5 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 will 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 asking the individual for an identification document. They also include using either of the options available to identify individuals who are not physically present. However, reasonable measures exclude any method that you believe would inform the individual that you are submitting a suspicious transaction report. See *Guideline 2: Suspicious Transactions* for more information.

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 How to ascertain the identity of an individual

See subsection 3.4 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, refer to 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 they want 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 used 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:

- 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 for client identification, 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.

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 conducting of a transaction, your agent or mandatary can also use the options explained below.

Individual not physically present

Most of the time in your business, your client is present when you have to ascertain their identity (for example, for a large cash transaction) and therefore, you have to use an identification document (as explained at the beginning of subsection 4.5).

In the case of a suspicious transaction, you may not be able to ascertain the identity of the individual because, for example, you believe that doing so would inform the client that you are submitting a suspicious transaction report. In this situation, you could use the methods described below to identify the individual.

To ascertain the identity of an individual who is not physically present, 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 purchasing gold from 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 client's identity 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 either of the following methods, but you cannot combine them:

- 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 enable verification of 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.

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. This 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 either of the following methods, but you cannot combine them.

- 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. You could do this by viewing an original bank statement.

For either method, the account has to be with a financial entity. For a definition of a financial entity, please see subsection 3.2.

The account cannot be one that is exempt from identification requirements for the financial entity, such as a registered retirement savings plan or a reverse mortgage. For more information about accounts that cannot be used for the cleared cheque or deposit account methods, see *Guideline 6G: Record Keeping and Client Identification for Financial Entities*.

4.6 Keeping client identification information up to date

Your compliance program 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, in high-risk situations, you will have to take measures to keep client identification information up to date, as part of your obligation to adopt enhanced measures for high-risk clients.

In this context, measures to keep client identification information up to date include asking the client to provide information in order that you can confirm or update 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.

5 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.

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).

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.

For dealers in precious metals and stones, the business relationship only includes transactions and related activities for which you have to ascertain the identity of your client. However, when you have to send a suspicious transaction report, you must still take reasonable measures to ascertain the identity of the client even if the transaction in question does not normally require it. See section 4 for more information on these transactions and activities.

If you have a client who conducts two or more suspicious transactions, even if you are unable to ascertain the identity of the client, you have still entered a business relationship with 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 enhanced measures (as required for all your high-risk business relationships) which include monitoring the business relationship for the purpose of reporting suspicious transactions, updating the client identification information, and taking any other appropriate enhanced measures to mitigate risk.

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.

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.

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.

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 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:

- Purchasing or selling jewellery
- Purchasing or selling precious metals (for example, gold, silver, platinum, or palladium)
- Purchasing or selling precious stones (for example, diamonds, sapphires, emeralds, tanzanite, rubies, or alexandrite)

You are not required to perform ongoing monitoring or keep a record of monitoring activities for business relationships that are not high-risk. However, for **high-risk** business relationships, you are required to monitor the business relationship, take any other appropriate enhanced measures to mitigate risk (see examples above), and keep a record of these activities.

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

6 Third Party Determination and Related Records

6.1 Third party determination

You have to make a third party determination whenever you have to keep a large cash transaction record as explained 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. 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.

Reasonable measures

What constitutes reasonable measures 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.

6.2 Third party records

If you determine that there is in fact a third party who gave instructions to the individual conducting the transaction, 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
- the nature of the relationship between the third party and the individual who gives you the cash. 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 whether, according to the individual giving the cash, the transaction is being conducted 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.

7 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 a paper copy can be readily produced 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.

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 3.3), 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 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.

Large cash transactions 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.

8 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.

9 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.

10 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