

## **Guideline 2: Suspicious Transactions**

# Guideline 2: Suspicious Transactions

## March 24, 2003

This replaces the previous version of *Guideline 2: Suspicious Transactions* issued in May 2002. The changes made are indicated by a side bar to the right of the modified text.

### Table of Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>General</b> .....   | <b>4</b>  |
| <b>2</b> | <b>Suspicious Transaction Reporting</b> .....                  | <b>6</b>  |
| 2.1      | Who Must Report Suspicious Transactions? .....                 | 6         |
| 2.2      | What are Suspicious Transactions?.....                         | 7         |
| 2.3      | Completed Transactions.....                                    | 8         |
| 2.4      | How to Make a Suspicious Transaction Report.....               | 9         |
| 2.5      | Additional Information Related to Reporting to FINTRAC .....   | 9         |
| <b>3</b> | <b>Identifying Suspicious Transactions</b> .....               | <b>11</b> |
| 3.1      | How to Identify a Suspicious Transaction.....                  | 11        |
| 3.2      | Indicators Relating to Terrorist Activity Financing.....       | 11        |
| 3.3      | Indicators of Suspicious Transactions .....                    | 13        |
| <b>4</b> | <b>Examples of Common Indicators</b> .....                     | <b>14</b> |
| 4.1      | General.....   | 14        |
| 4.2      | Knowledge of Reporting or Record Keeping Requirements .....    | 14        |
| 4.3      | Identity Documents.....  | 15        |
| 4.4      | Cash Transactions .....  | 15        |
| 4.5      | Economic Purpose.....  | 16        |
| 4.6      | Transactions Involving Accounts .....                          | 16        |
| 4.7      | Transactions Involving Areas Outside Canada.....               | 17        |
| 4.8      | Transactions Related to Offshore Business Activity .....       | 17        |
| <b>5</b> | <b>Examples of Industry-Specific Indicators</b> .....          | <b>19</b> |
| 5.1      | Industry-Specific Indicators .....                             | 19        |
| 5.2      | Financial Entities.....  | 20        |
| 5.3      | Businesses who Send or Receive Electronic Funds Transfers..... | 23        |
| 5.4      | Businesses who Provide Loans .....                             | 25        |
| 5.5      | Life Insurance Companies, Brokers and Agents.....              | 26        |
| 5.6      | Securities Dealers.....  | 27        |

|          |  |           |
|----------|--|-----------|
| 5.7      | Foreign Exchange Dealers and Money Services Businesses ..... | 29        |
| 5.8      | Accountants.....   | 30        |
| 5.9      | Real Estate Brokers or Sales Representatives.....            | 31        |
| 5.10     | Casinos.....   | 32        |
| <b>6</b> | <b>Comments? .....</b>                                       | <b>33</b> |
| <b>7</b> | <b>How to Contact FINTRAC .....</b>                          | <b>33</b> |

# 1 General

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* requires reporting of suspicious transactions by the following persons and entities and their employees:

- financial entities (such as banks, credit unions, caisses populaires, trust and loan companies and agents of the Crown that accept deposit liabilities);
- life insurance companies, brokers and agents;
- securities dealers, portfolio managers and investment counsellors;
- persons engaged in the business of foreign exchange dealing;
- money services businesses (including alternative remittance systems, such as Hawala, Hundi, Chitti, etc.);
- Canada Post for money orders;
- accountants and accounting firms (when carrying out certain activities on behalf of their clients);
- real estate brokers or sales representatives (when carrying out certain activities on behalf of their clients); and
- casinos (including those authorized to do business in Canada, with a slot machine or roulette or card games, but excluding certain temporary charity casinos).

If you are one of these persons or entities, this guideline can help you meet your obligation to report suspicious transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence.

This guideline, which has been prepared by FINTRAC, contains indicators of suspicious transactions that might be useful in helping you assess whether a transaction is suspicious and should be reported. It is not intended as a substitute for your own assessment, based on your knowledge and experience as well as the specific circumstances of the financial transaction.

This guideline uses plain language to explain common reporting 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. For more information about money laundering, terrorist activity financing or other reporting requirements under the Act and Regulations, 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 when and how to submit reports.
- *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*.
- *Guideline 5: Submitting Terrorist Property Reports to FINTRAC* explains to reporting persons and entities when and how to submit a terrorist property report.
- *Guideline 6: Record Keeping and Client Identification* explains the requirement for reporting persons and entities to identify their clients and keep records. There are eight different versions of Guideline 6, by sector.
- *Guideline 7: Submitting Large Cash Transaction Reports to FINTRAC* explains when and how to submit large cash transaction reports.
- *Guideline 8: Submitting Electronic Funds Transfer Reports to FINTRAC* explains when and how to submit EFT reports.

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 these guidelines, several references are provided to additional information that may be available on external Web sites. FINTRAC is not responsible for the accuracy or reliability of the information contained on those external Web sites.

## 2 Suspicious Transaction Reporting

### 2.1 Who Must Report Suspicious Transactions?

If you are a **reporting person or entity** mentioned above, you must report suspicious transactions to FINTRAC.

If you are a money services business, a Crown agent, an accountant, a real estate broker or sales representative, or a casino, you are only subject to this when you engage in the following activities:

- If you are a **money services business**, you are subject to this when you remit or transmit funds by any means through any person, entity or electronic funds transfer network. You are also subject to this when you issue or redeem money orders, traveller's cheques or other similar negotiable instruments, except when you redeem cheques payable to a named person or entity.

Money services businesses include alternative money remittance systems, such as Hawala, Hundi, Chitti, etc. Money services businesses also include financial entities when they remit or transmit funds, issue or redeem money orders, traveller's cheques or other similar negotiable instruments for anyone who is not a client of theirs.

- If you are an **agent of the Crown** (i.e., a Department or agent of her Majesty in right of Canada or of a province), you are subject to this when you sell or redeem money orders, such as Canada Post for example, or when you accept deposit liabilities in the course of providing financial services to the public.
- If you are an **accountant or an accounting firm**, you are subject to this when you receive professional fees to engage in any of the following activities on behalf of any person or entity (other than your employer), or to give instructions in respect of those activities on behalf of any person or entity (other than your employer):
  - receiving or paying funds;
  - purchasing or selling securities, real property or business assets or entities;
  - or
  - transferring funds or securities by any means.

These accountant activities do not include audit, review or compilation work carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook.

- If you are a **real estate broker or sales representative**, you are subject to this when you engage in any of the following activities on behalf of any person or entity in the course of a real estate transaction:
  - receiving or paying funds;
  - depositing or withdrawing funds; or
  - transferring funds by any means.
- If you are a **casino** authorized to do business in Canada, you are subject to this if roulette or card games are carried on in your establishment, or if your establishment has a slot machine. In this context, a slot machine does not include a video lottery terminal.

If you are a registered charity, you may be authorized to do business only temporarily as a casino for charitable purposes. If this is your situation, and you carry on business in the casino for two consecutive days or less under the supervision of an employee of the casino, you are not subject to this.

## 2.2 What are Suspicious Transactions?

Suspicious transactions are financial transactions that there are reasonable grounds to suspect are related to the commission of a **money laundering offence**. Since June 12, 2002, suspicious transactions also include financial transactions that there are reasonable grounds to suspect are related to the commission of a **terrorist activity financing offence**.

“Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within your industry. While the Act and Regulations do not specifically require you to implement or use an automated system for detecting suspicious transactions, you may decide that such a system would be beneficial to your business.

More information about a money laundering offence and terrorist activity financing offences is provided below.

### **Money Laundering Offence**

Under Canadian law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means most serious offences under the *Criminal Code* or any other federal Act. It includes those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, etc. The few exceptions are for offences such as those related to tax evasion or breach of copyright, and some others that involve administrative and monetary penalty structure.

A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Canada.

For information about money laundering methods, see *Guideline 1: Backgrounder*.

### **Terrorist Activity Financing Offence**

Under Canadian law, terrorist activity financing offences make it a crime to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorist crimes. This includes inviting someone else to provide property for this purpose. It also includes the use or possession of property to facilitate or carry out terrorist activities.

There are other offences associated with terrorist activities that are not specifically related to financing, such as participating in or facilitating terrorist activities, or instructing and harbouring terrorists. Only suspicion that a transaction is related to a terrorist activity financing offence triggers a requirement to report the suspicious transaction to FINTRAC as related to terrorist activity financing.

For more information about terrorist financing and other anti-terrorism measures, including other reporting requirements related to terrorist property, see *Guideline 1: Backgrounder*.

## **2.3 Completed Transactions**

The requirement for you to report a suspicious transaction applies only when the financial transaction has occurred. For example, if you process a deposit from a client, a financial transaction has occurred, even if the final sale does not go through. In this example, the refund of the deposit would also be a financial transaction. If you decide or the client decides not to complete the transaction, there is no obligation to report it as a suspicious transaction to FINTRAC.

You could choose to report an uncompleted transaction and your suspicion about it to law enforcement. You could also choose to provide this information voluntarily to FINTRAC. To find out how to provide information voluntarily to FINTRAC about suspicions of money laundering or of the financing of terrorist activities, refer to FINTRAC's Web site at [http://www.fintrac.gc.ca/reporting--declaration/vol/1\\_e.asp](http://www.fintrac.gc.ca/reporting--declaration/vol/1_e.asp).

### **Transactions Related to Terrorist Property**

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

This could occur, for example, if your concern about the transaction is because you know that the property in question is owned or controlled by or on behalf of a listed person or listed entity (that is, someone believed to be involved in terrorist activity). For more

information about listed persons or entities, freezing of property, and the associated reporting requirement to FINTRAC, read Section 4.2 of *Guideline 1: Background*.

## **2.4 How to Make a Suspicious Transaction Report**

Once you have detected a fact that leads you to have reasonable grounds to suspect that a transaction is related to the commission of a money laundering offence or to the commission of a terrorist activity financing offence, a suspicious transaction report must be sent to FINTRAC within 30 days.

Please refer to *Guideline 3: Submitting Suspicious Transaction Reports to FINTRAC* for more information about reporting timelines and for information on how to make a report.

Making a suspicious transaction report to FINTRAC does not prevent you from reporting suspicions of money laundering or terrorist financing directly to law enforcement. FINTRAC encourages you to maintain established relationships with law enforcement.

## **2.5 Additional Information Related to Reporting to FINTRAC**

### **Confidentiality**

As a reporting person or entity, you are not allowed to inform anyone, including the client, about the contents of a suspicious transaction report or even that you have made such a report, if your intent is to harm or impair a criminal investigation. This applies whether or not such an investigation has begun.

Because it is important not to tip your client off that you are making a suspicious transaction report, you should not be requesting information that you would not normally request during a transaction. The fields that are mandatory in the suspicious transaction report are for information without which you should not be able to complete a transaction. The rest of the fields are for you to provide information if it is available in your records or as a result of the transaction.

Since June 12, 2002, there are new client identification and record keeping requirements. More information about these is available in *Guideline 4: Implementation of a Compliance Regime* or *Guideline 6: Record Keeping and Client Identification*.

### **Immunity**

No criminal or civil proceedings may be brought against you for making a report in good faith concerning a suspicious transaction. This also applies if you are not required to submit a report to FINTRAC, but decide to provide information voluntarily to FINTRAC because of your suspicions of money laundering or financing of terrorist activity.

### **Penalties**

There are penalties if you fail to meet the suspicious transaction reporting obligations. Failure to report a suspicious transaction could lead to up to five years imprisonment, a

fine of \$2,000,000, or both. However, penalties for failure to report do not apply to employees who report suspicious transactions to their superior.

### **Closing Accounts**

There is no requirement under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to close a client's account when you have reported or are preparing to report a suspicious transaction. This is entirely up to you and your business practices.

## 3 Identifying Suspicious Transactions

### 3.1 How to Identify a Suspicious Transaction

Transactions may give rise to reasonable grounds to **suspect** that they are related to money laundering or terrorist activity financing regardless of the sum of money involved. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission of a money laundering offence, a terrorist activity financing offence, or both.

As a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

The context in which the transaction occurs is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. As a reporting person or entity, or an employee of a reporting person or entity, you should evaluate transactions in terms of what seems appropriate and is within normal practices in your particular line of business, and based on your knowledge of your client. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. Remember that **behaviour** is suspicious, not people. Also, it could be the consideration of many factors—not just one factor—that will lead you to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering offence, a terrorist activity financing offence, or both. All circumstances surrounding a transaction should be reviewed.

As the reporting person or entity with whom the transaction occurs, you have to assess whether there are reasonable grounds to suspect that a transaction is related to a money laundering offence or a terrorist activity financing offence. The following information concerning indicators is provided to help you with this.

### 3.2 Indicators Relating to Terrorist Activity Financing

Indicators to help establish suspicion that a transaction may be related to the commission of a terrorist activity financing offence mostly resemble those relating to money laundering. In fact, the indicators in this guideline are combined for both money laundering and terrorist financing. These are all intended to complement each other and reinforce already existing due diligence practices in dealing with financial transactions.

There are some small differences between money laundering and terrorist financing indicators. For example, amounts relating to terrorist financing generally may be smaller. However, there is no distinction made in the indicators included in Sections 4 and 5 below.

### **Lists of persons and entities believed to be associated with terrorists**

As part of international efforts to combat terrorism, the Government of Canada has published lists to prevent and suppress the financing of terrorist activities. Property of those whose names are published on any of these anti-terrorism lists are to be frozen. This means that transactions related to that property are prohibited.

A consolidated list for use by anyone in Canada and by Canadians outside Canada is published and maintained by the Office of the Superintendent of Financial Institutions (OSFI). You can find this list on OSFI's Web site: [http://www.osfi-bsif.gc.ca/eng/publications/advisories/index\\_supervisory.asp?#Supter](http://www.osfi-bsif.gc.ca/eng/publications/advisories/index_supervisory.asp?#Supter)

If you determine that you are in control or possession of property that is owned by or on behalf of anyone on this list, you must report its existence, as well as any transactions or proposed transactions related to the property, to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service. Please refer to *Guideline 1: Background* for more information about this.

Others outside Canada, such as the United States, the United Nations Security Council, among others, have also published lists. Some or all of the names on these foreign lists may also be added on the Canadian lists, if Canada has reasonable grounds to believe they are associated to terrorist activity.

### **How to use lists as indicators of possible terrorist activity financing**

If you know that the transaction is related to property owned or controlled by or on behalf of anyone whose name is on the lists, the property should be frozen. This means that any transactions relating to that property are prohibited. Therefore, such a transaction that would trigger suspicion about a terrorist activity financing offence should not be completed.

Because of this, and because the requirement to report a suspicious transaction only exists if a transaction is completed, it is expected that the number of transactions that could give rise to a suspicious transaction report related to terrorist activity financing will be limited. For more information about proposed transactions related to terrorist property, read Section 4.2 of *Guideline 1: Background*.

### **Distinguishing between money laundering and terrorist activity financing suspicion**

It may be difficult for you to distinguish between suspicion of money laundering and suspicion of terrorist activity financing. In fact, it is possible that a transaction could be related to both. For example, funds to be used for terrorist activity could be proceeds of criminal activity as well as from legitimate sources.

It is the information about the transaction and about what led to your suspicion that is important in a suspicious transaction report. Provide as many details as possible in your report about what led to your suspicion, including anything that made you suspect that it might be related to terrorist financing, money laundering, or both. If you cannot make the distinction based on the information available, remember that it is the information about your suspicion that is important, not the distinction between money laundering and terrorist activity offences.

### **3.3 Indicators of Suspicious Transactions**

The indicators that follow are provided to help assess whether or not transactions might give rise to reasonable grounds for suspicion. They are examples of common and industry-specific indicators that may be helpful when evaluating transactions. They include indicators based on certain characteristics that have been linked to money laundering or terrorist activities in the past.

These indicators were compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations. They are not intended to cover every possible situation and are not to be viewed in isolation. A single indicator is not necessarily indicative of reasonable grounds to suspect money laundering or terrorist financing activity. However, if a number of indicators are present during a transaction or series of transactions, then you might want to take a closer look at other factors prior to making the determination as to whether the transaction must be reported.

The indicators have to be assessed in the context in which the transaction occurs. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence. However, it may also offer no indication of this in view of factors such as the client's occupation, business, financial history and past investment pattern. Taken together, the presence of one or more indicators as well as your knowledge of your client's business or financial affairs may help you identify suspicious transactions.

Some of the indicators provided could result in the transaction being aborted if the client requests a service that is prohibited by your business or by the anti-terrorism measures explained in Section 4.2 of *Guideline 1: Background*. Your policies, standards and procedures may already reflect these as inappropriate or questionable. As explained earlier, if a transaction is not completed, there is no requirement for you to make a suspicious transaction report to FINTRAC. However, the indicators detected during an aborted transaction should be considered, where possible, in subsequent dealings with the client if additional suspicious activity occurs.

In the case of a transaction aborted because you believe the property is owned or controlled by or on behalf of a terrorist or a terrorist group, this must be reported as explained in Section 3.2 above.

## **4 Examples of Common Indicators**

The following are examples of common indicators that may point to a suspicious transaction. Please read Section 3 (above) for general information about identifying suspicious transactions and how to use these indicators.

### **4.1 General**

- Client admits or makes statements about involvement in criminal activities.
- Client does not want correspondence sent to home address.
- Client appears to have accounts with several financial institutions in one area for no apparent reason.
- Client repeatedly uses an address but frequently changes the names involved.
- Client is accompanied and watched.
- Client shows uncommon curiosity about internal systems, controls and policies.
- Client has only vague knowledge of the amount of a deposit.
- Client presents confusing details about the transaction.
- Client over justifies or explains the transaction.
- Client is secretive and reluctant to meet in person.
- Client is nervous, not in keeping with the transaction.
- Client is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after opening account.
- Client is involved in activity out-of-keeping for that individual or business.
- Client insists that a transaction be done quickly.
- Inconsistencies appear in the client's presentation of the transaction.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client uses aliases and a variety of similar but different addresses.
- Client uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Client offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- You are aware that a client is the subject of a money laundering or terrorist financing investigation.

### **4.2 Knowledge of Reporting or Record Keeping Requirements**

- Client attempts to convince employee not to complete any documentation required for the transaction.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client has unusual knowledge of the law in relation to suspicious transaction reporting.
- Client seems very conversant with money laundering or terrorist activity financing issues.

- Client is quick to volunteer that funds are “clean” or “not being laundered.”

### **4.3 Identity Documents**

- Client provides doubtful or vague information.
- Client produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Client refuses to produce personal identification documents.
- Client only submits copies of personal identification documents.
- Client wants to establish identity using something other than his or her personal identification documents.
- Client’s supporting documentation lacks important details such as a phone number.
- Client inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.

### **4.4 Cash Transactions**

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Client frequently exchanges small bills for large ones.
- Client uses notes in denominations that are unusual for the client, when the norm in that business is much smaller or much larger denominations.
- Client presents notes that are packed or wrapped in a way that is uncommon for the client.
- Client deposits musty or extremely dirty bills.
- Client makes cash transactions of consistently rounded-off large amounts (e.g., \$9,900, \$8,500, etc.).
- Client consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Client consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Client presents uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which could trigger reporting requirements.
- Client conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Client frequently purchases traveller’s cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the client.
- Client asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.)

- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

#### **4.5 Economic Purpose**

- Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the client.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

#### **4.6 Transactions Involving Accounts**

- Opening accounts when the client's address is outside the local service area.
- Opening accounts in other people's names.
- Opening accounts with names very close to other established business entities.
- Attempting to open or operating accounts under a false name.
- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Client frequently uses many deposit locations outside of the home branch location.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Activity far exceeds activity projected at the time of opening of the account.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly sees significant activity.
- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Unexplained transfers between the client's products and accounts.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.
- Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities. More information on which countries these characteristics may apply to can be found at the following Web sites:

[http://www1.oecd.org/fatf/NCCT\\_en.htm](http://www1.oecd.org/fatf/NCCT_en.htm) (information from the Financial Action Task Force about non-cooperative countries and territories in the fight against money laundering and terrorist financing)  
[http://www.state.gov/www/global/narcotics\\_law/1999\\_narc\\_report/index.html](http://www.state.gov/www/global/narcotics_law/1999_narc_report/index.html) (International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2000)  
[http://www.fintrac.gc.ca/publications/avs/2002-12-20\\_e.asp](http://www.fintrac.gc.ca/publications/avs/2002-12-20_e.asp)

#### **4.7 Transactions Involving Areas Outside Canada**

- Client and other parties to the transaction have no apparent ties to Canada.
- Transaction crosses many international lines.
- Use of a credit card issued by a foreign bank that does not operate in Canada by a client that does not live and work in the country of issue.
- Transactions involving countries deemed by the Financial Action Task Force as requiring enhanced surveillance, including the Republic of Nauru.
- Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country known for highly secretive banking and corporate law.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.
- Transaction involves a country known or suspected to facilitate money laundering activities.

More information on which countries these characteristics (i.e. those mentioned in the last two bullets) may apply to can be found at the following Web sites:

[http://www1.oecd.org/fatf/NCCT\\_en.htm](http://www1.oecd.org/fatf/NCCT_en.htm) (information from the Financial Action Task Force about non-cooperative countries and territories in the fight against money laundering and terrorist financing)  
[http://www.state.gov/www/global/narcotics\\_law/1999\\_narc\\_report/index.html](http://www.state.gov/www/global/narcotics_law/1999_narc_report/index.html) (International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2000)  
[http://www.fintrac.gc.ca/publications/avs/2002-12-20\\_e.asp](http://www.fintrac.gc.ca/publications/avs/2002-12-20_e.asp)

#### **4.8 Transactions Related to Offshore Business Activity**

Any person or entity that conducts transactions internationally should consider the following indicators.

- Accumulation of large balances, inconsistent with the known turnover of the client's business, and subsequent transfers to overseas account(s).

- Frequent requests for traveller's cheques, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transfers by client on an in-and-out basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the client's business.
- Use of a credit card issued by an offshore bank.

## 5 Examples of Industry-Specific Indicators

### 5.1 Industry-Specific Indicators

In addition to the general indicators outlined above, the following industry-specific indicators may point to a suspicious transaction. Remember that **behaviour** is suspicious, not people. Also, it is the consideration of many factors—not any one factor—that will lead to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence. All circumstances surrounding a transaction should be reviewed, within the context of your knowledge of your client.

Taken together, the general and industry-specific indicators that apply to your business may help you identify suspicious transactions. Depending on the services you provide, you may need information about indicators in more than one of the following sections. For example, if you are a financial advisor, you might sell life insurance products and securities. In this case, you would read the indicators in Section 5.5 (Life Insurance Companies, Brokers and Agents), as well as under Section 5.6 (Securities Dealers).

## 5.2 Financial Entities

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators.

The following indicators are for your consideration if you are an institution that opens accounts and holds deposits on behalf of individuals or companies. This includes banks, credit unions, caisses populaires, trust and loan companies and agents of the Crown that accept deposit liabilities.

### Personal Transactions

- Client appears to have accounts with several financial institutions in one geographical area.
- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- Client makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account).
- Client runs large credit card balances.
- Client visits the safety deposit box area immediately before making cash deposits.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her address.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client deposits large endorsed cheques in the name of a third-party.
- Client frequently makes deposits to the account of another person who is not an employer or family member.
- Client frequently exchanges currencies.
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Client's access to the safety deposit facilities increases substantially or is unusual in light of their past usage.
- Many unrelated individuals make payments to one account without rational explanation.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.
- Client acquires significant assets and liquidates them quickly with no explanation.
- Client acquires significant assets and encumbers them with security interests that don't make economic sense.

## Corporate and Business Transactions

Some businesses may be susceptible to the mixing of illicit funds with legitimate income. This is a very common method of money laundering. These businesses include those that conduct the majority of their business in cash, such as restaurants, bars and vending machine companies. On opening accounts with the various businesses in your area, you would likely be aware of those that are mainly cash based. Unusual or unexplained increases in cash deposits made by those entities may be indicative of suspicious activity.

- Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc.
- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of monetary instruments that are atypical of legitimate business activity (for example, deposits that include a mix of business, payroll, and social security cheques).
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Business does not want to provide complete information regarding its activities.
- Financial statements of the business differ noticeably from those of similar businesses.
- Representatives of the business avoid contact with the branch as much as possible, even when it would be more convenient for them.
- Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations.
- Client maintains a number of trustee or client accounts that are not consistent with that type of business or not in keeping with normal industry practices.
- Client operates a retail business providing cheque-cashing services but does not make large draws of cash against cheques deposited.
- Client pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments.
- Client purchases cashier's cheques and money orders with large amounts of cash.
- Client deposits large amounts of currency wrapped in currency straps.
- Client makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere.
- Client makes a large volume of cash deposits from a business that is not normally cash-intensive.
- Client makes large cash withdrawals from a business account not normally associated with cash transactions.
- Client consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad.
- Client makes a single and substantial cash deposit composed of many large bills.
- Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business.

- There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred.
- There is a sudden change in cash transactions or patterns.
- Client wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business.
- There is a marked increase in transaction volume on an account with significant changes in an account balance that is inconsistent with or not in keeping with normal business practices of the client's account.
- Asset acquisition is accompanied by security arrangements that are not consistent with normal practice.
- Unexplained transactions are repeated between personal and commercial accounts.
- Activity is inconsistent with stated business.
- Account has close connections with other business accounts without any apparent reason for the connection.
- Activity suggests that transactions may offend securities regulations or the business prospectus is not within the requirements.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

### **5.3 Businesses who Send or Receive Electronic Funds Transfers**

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are involved in the business of electronic funds transfers, consider the following indicators.

- Client orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Client transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash.
- Client receives large sums of money from an overseas location via electronic funds transfer that includes instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Client receives electronic funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the client.
- Client requests payment in cash immediately upon receipt of a large electronic funds transfer.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.
- Client transfers funds to another country without changing the form of currency.
- Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities having no apparent business connection with client.
- Size of electronic transfers is out-of-keeping with normal business transactions for that client.
- Wire transfers do not have information about the beneficial owner or originator when the inclusion of this information would be expected.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).
- Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.

- Client conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices.
- Client makes electronic funds transfers to free trade zones that are not in line with the client's business.

More information on which countries these characteristics may apply to can be found at the following Web sites:

[http://www.state.gov/www/global/narcotics\\_law/1999\\_narc\\_report/index.html](http://www.state.gov/www/global/narcotics_law/1999_narc_report/index.html)

(International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2000)

## **5.4 Businesses who Provide Loans**

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are involved in the business of providing loans or extending credit to individuals or corporations, consider the following indicators.

- Client suddenly repays a problem loan unexpectedly.
- Client's employment documentation lacks important details that would make it difficult for you to contact or locate the employer.
- Client has loans to or from offshore companies that are outside the ordinary course of business of the client.
- Client offers you large dollar deposits or some other form of incentive in return for favourable treatment on loan request.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- Client applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the client.

## **5.5 Life Insurance Companies, Brokers and Agents**

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you provide life insurance as your main occupation or as one of the many services that you offer, consider the following indicators.

- Client proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account.
- Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump payment.
- Client conducts a transaction that results in a conspicuous increase in investment contributions.
- Client cancels investment or insurance soon after purchase.
- Client shows more interest in the cancellation or surrender than in the long-term results of investments.
- Client makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment.
- The duration of the life insurance contract is less than three years.
- The first (or single) premium is paid from a bank account outside the country.
- Client accepts very unfavourable conditions unrelated to his or her health or age.
- Transaction involves use and payment of a performance bond resulting in a cross border payment.

## 5.6 Securities Dealers

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are involved in the business of dealing in securities or segregated fund products, including portfolio managers and investment counsellors, consider the following indicators.

- A new or prospective client is known to you as having a questionable legal reputation or criminal background.
- Normal attempts to verify the background of a new or prospective client are difficult.
- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than \$10,000, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.
- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in stocks, bonds, investment trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large dollar size.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of Canada.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the client.

- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by, or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of persons other than the client.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

More information on which countries these characteristics may apply to can be found at the following Web site: [http://www1.oecd.org/fatf/NCCT\\_en.htm](http://www1.oecd.org/fatf/NCCT_en.htm) (information from the Financial Action Task Force about non-cooperative countries and territories in the fight against money laundering and terrorist financing)

## 5.7 Foreign Exchange Dealers and Money Services Businesses

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are involved in the money services business, including foreign exchange dealers, money remitters, issuers of traveller's cheques and post offices, consider the following indicators.

- Client requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Client wants to pay transaction fees that exceed the posted fees.
- Client exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Client knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Client wants a cheque issued in the same currency to replace the one being cashed.
- Client wants cash converted to a cheque and you are not normally involved in issuing cheques.
- Client wants to exchange cash for numerous postal money orders in small amounts for numerous other parties.
- Client enters into transactions with counter parties in locations that are unusual for the client.
- Client instructs that funds are to be picked up by a third party on behalf of the payee.
- Client makes large purchases of traveller's cheques not consistent with known travel plans.
- Client requests numerous cheques in small amounts and various names, which total the amount of the exchange.
- Client requests that a cheque or money order be made out to the bearer.
- Client requests that a large amount of foreign currency be exchanged to another foreign currency.

## 5.8 Accountants

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are an accountant, consider the following indicators when you are carrying out certain activities on behalf of your client, as explained in Section 2.1.

- Client appears to be living beyond his or her means.
- Client has business activity inconsistent with industry averages or financial ratios.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

More information on which countries these characteristics may apply to can be found at the following Web site: <http://www.oecd.org/EN/document/0,,EN-document-103-3-no-4-4393-103,00.html>(Organisation for Economic Co-Operation and Development tax haven update information)

## 5.9 Real Estate Brokers or Sales Representatives

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are in the real estate industry, consider the following indicators when carrying out certain activities on behalf of your clients, as explained in Section 2.1.

- Client arrives at a real estate closing with a significant amount of cash.
- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table".
- Client sells property below market value with an additional "under the table" payment.
- Client pays initial deposit with a cheque from a third party, other than a spouse or a parent.
- Client pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Client purchases personal use property under corporate veil when this type of transaction is inconsistent with the ordinary business practice of the client.
- Client purchases property without inspecting it.
- Client purchases multiple properties in a short time period, and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Client is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided.

## 5.10 Casinos

Please read Section 3 and Section 5.1 (above) for general information about identifying suspicious transactions and how to use these indicators. If you are engaged in the casino business, consider the following indicators.

- Any casino transaction of \$3,000 or more when an individual receives payment in casino cheques made out to third parties or without a specified payee.
- Client requests a winnings cheque in a third party's name.
- Acquaintances bet against each other in even-money games and it appears that they are intentionally losing to one of the party.
- Client attempts to avoid the filing of a report for cash by breaking up the transaction.
- Client requests cheques that are not for gaming winnings.
- Client enquires about opening an account with the casino and the ability to transfer the funds to other locations when you do not know the client as a regular, frequent or large volume player.
- Client purchases large volume of chips with cash, participates in limited gambling activity with the intention of creating a perception of significant gambling, and then cashes the chips for a casino cheque.
- Client exchanges small denomination bank notes for large denomination bank notes, chip purchase vouchers or cheques.
- Client is known to use multiple names.
- Client requests the transfer of winnings to the bank account of a third party or a known drug source country or to a country where there is no effective anti-money-laundering system.

More information on which countries these characteristics may apply to can be found at the following Web sites:

[http://www.state.gov/www/global/narcotics\\_law/1999\\_narc\\_report/index.html](http://www.state.gov/www/global/narcotics_law/1999_narc_report/index.html)  
(International Narcotics Control Strategy Report released by the Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2000)

[http://www1.oecd.org/fatf/NCCT\\_en.htm](http://www1.oecd.org/fatf/NCCT_en.htm) (information from the Financial Action Task Force about non-cooperative countries and territories in the fight against money laundering and terrorist financing)

## **6 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@fintrac.gc.ca](mailto:guidelines@fintrac.gc.ca)

## **7 How to Contact FINTRAC**

For further information on FINTRAC and its activities, or about reporting suspicious transactions, please go to FINTRAC's Web site (<http://www.fintrac.gc.ca>) or contact FINTRAC:

Financial Transactions and Reports Analysis Centre of Canada  
234 Laurier Avenue West, 24<sup>th</sup> floor  
Ottawa, Ontario  
Canada K1P 1H7

Toll-free: 1-866-346-8722