

Anti-Money Laundering Compliance Guide

Proceeds of Crime
(Money Laundering) &
Terrorist Financing Act
(PCMLTFA)



Reporting Requirements

Recordkeeping

FINTRAC Resources

Employee Training



Dear MoneyGram Agent:

The purpose of this Guide is to help you and your employees:


- Detect and prevent money laundering and terrorist financing;
- Comply with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) recordkeeping and reporting requirements;
- Comply with federal anti-terrorism and sanctions laws and regulations; and
- Identify and report suspicious activity.

Your knowledge of the information in this Guide may help prevent your business from being victimized by money launderers and help you comply with the law. In addition, your compliance with these requirements may help law enforcement agents in their efforts to track down and capture terrorists who illegally launder money.

It is MoneyGram's policy to follow the spirit, as well as the letter of the law. We do not want our money transfer services to be used for illegal purposes. We will not do business with anyone who knowingly violates the law. Although we cannot take responsibility for you or your employees' compliance with the anti-money laundering laws and regulations, we believe this Guide can help you develop your own effective anti-money laundering compliance program.

This Guide provides a general description of the PCMLTFA requirements as they may relate to MoneyGram money transfers and should not be considered to cover all possible situations; there may be other PCMLTFA requirements that apply to other facets of your business. There are other requirements that apply to the redemption of money orders, the issuance and redemption of traveller's cheques and cheque cashing. There are also separate requirements that apply to foreign exchange dealers.

MoneyGram thanks you for your shared dedication to the fight against money laundering and terrorism.





Guide Contents

Section I. Money Laundering Overview

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money.

Section II. MSB Registration

All money services businesses in Canada must register as MSBs. MoneyGram agents are covered by MoneyGram's registration unless your business conducts MSB activity outside of our agent relationship.

Section III. PCMLTFA Compliance Regime

We require that you to implement an anti-money laundering regime based on the risks associated with your business, such as size, location, volume of business, etc.

Section IV. Recordkeeping

You must record information regarding MoneyGram money transfer transactions of \$1,000 or more.

Section V. Transaction Reporting

The Large Cash Transaction Report (LCTR) must be filed on all cash transactions of \$10,000 or more requested by or on behalf of the same person in a 24-hour period. The Electronic Fund Transfer report must be filed on all international money transfers of \$10,000 or more conducted by or on behalf of the same person in a 24-hour period. MGI files these reports for our agents.

Section VI. Structuring

Structuring is the illegal act of breaking up a larger transaction into smaller transactions in order to avoid the recordkeeping or reporting requirements.

Section VII. Reporting Suspicious Activity

The Suspicious Transaction Report (STR) must be filed on all suspicious transactions. Suspicious activity involves transactions or attempted transactions that appear to be structured or do not have any legitimate purpose.

Section VIII. Anti-Terrorist / Sanctions Legislation

You cannot deal with any property if you know it is owned or controlled by a terrorist or terrorist group.

Section IX. Civil and Criminal Penalties

The government requires strict compliance with all anti-money laundering rules and regulations. If you do not comply, you may be subject to large fines and / or imprisonment.



Section I.

Money Laundering Overview

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money.

This definition covers a wide range of activity and is not limited to cash or currency transactions. Money laundering can involve any type of money, including money orders, money transfers and other financial transactions. You need to understand how people launder money so that you can identify money laundering and know how to help prevent it.

To help prevent the laundering of cash and to obtain documentation that may be used to prosecute money launderers, the government requires you to maintain records on certain cash transactions. Some transactions also require that reports be filed and maintained.

Who is covered?

Because you process money transfers, you are subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*, the *Criminal Code*, the *United Nations Act*, and other anti-money laundering / anti-terrorism laws.

Section II.

Money Services Business (MSB) Registration

The PCMLTFA requires money services businesses (MSBs) to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

A MSB is an individual or entity engaged in the business of any of the following:

- Foreign exchange dealing;
- Remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network; or
- Issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity.

MoneyGram agents are covered by MoneyGram's registration unless your business conducts MSB activity outside of our agent relationship.

Alternative money remittance systems such as Hawala, Hundi or Chitti must register as MSBs; all foreign exchange services must register separately, even if they are a MoneyGram agent.



Section III.

PCMLTFA Compliance Regime

The PCMLTFA requires that all MSBs adopt a Compliance Regime to guard against money laundering and/or terrorist financing. MoneyGram requires all agents in Canada to adopt a customized Compliance Regime. MoneyGram has a Compliance Regime to comply with the PCMLTFA that can be customized for your use.

Your compliance regime must be tailored to fit your circumstance and needs; it should reflect the nature, size and complexity of your business.

Your Compliance Regime must include the following:

- A.** The designation of a Compliance Officer who is responsible for assuring that:
 - A Risk Assessment is conducted;
 - Policies and procedures are followed;
 - Procedures are updated as needed; and
 - Training and education are provided.

- B.** Internal documented policies, procedures and controls for:
 - Verifying client identification;
 - Filing reports;
 - Creating and retaining records; and
 - Risk assessment and mitigation.

- C.** An ongoing documented employee training program that:
 - Explains policies and procedures; and
 - Teaches how to identify suspicious activity

- D.** An independent review of your anti-money laundering regime.
 - The review should take place every two (2) years and be as thorough as needed based on the risks specific to your business; and
 - The review may be performed by one of your employees, but cannot be performed by your Compliance Officer.

The information contained in this guide provides your business with the tools it needs to build an anti-money laundering regime. However, the quality and effectiveness of your regime depends on your commitment to it.



Establishing an Effective Compliance Regime:

First, your business should designate a Compliance Officer. The Compliance Officer may be an employee who has other duties at your business, but it should be someone in a responsible position. The Compliance Officer is responsible for your business's day-to-day compliance with the anti-money laundering laws and anti-terrorism laws and sanctions and for ensuring the compliance regime is updated as needed. The Compliance Officer is also responsible for conducting a risk assessment and overseeing your business's ongoing education and training program.

Second, your business should formally adopt an anti-money laundering compliance regime. This Guide can serve as the basis for that regime. An easy to use template titled the *CANADIAN ANTI-MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION COMPLIANCE REGIME* can also be downloaded from the Anti-Money Laundering page at www.moneygram.com to create a customized Compliance Regime for your business.

Third, your business should establish an ongoing employee-training program for all employees who will have any involvement with MSB activities. The educations and training should include instruction on the employees' training in this Guide. All employees should be required to read this Guide prior to conducting any MSB transactions. In addition, prior to conducting any MSB transactions, employees should sign your Compliance Regime or another form of training documentation that is kept in their personnel file. Employees should also receive periodic updates to their training, particularly when there are changes in regulations. Please refer to the Anti-Money Laundering page at www.moneygram.com for additional resources to help train your employees.

Fourth, your business should subject your anti-money laundering compliance regime to an independent review to assure its adequacy. The scope and frequency of this review should be adjusted to allow for the risk of the financial services provided by your business. This review may be conducted by an officer or employee of your business, but it should not be conducted by the person who is designated as the Compliance Officer.

Finally, it is important that you create recordkeeping files for your Compliance Regime. These files should be readily accessible if your business is examined/audited by regulators.

Question: Where can an Agent get more information concerning the PCMLTFA?

This Agent Compliance Guide is only a general description of the PCMLTFA requirements as they may relate to the MoneyGram products. The FINTRAC website contains additional information regarding the PCMLTFA at: www.fintrac.gc.ca.



Section IV.

Recordkeeping

Both sending and receiving agents must obtain and record specific information for money transfers of \$1,000 or more regardless of the method of payment. Your client must be physically present in your location when conducting a transaction so that you can obtain and verify the client's identifying information.

MoneyGram will not process any transaction if the client is not physically present at a MoneyGram location. Only person-to-person transactions are allowed.

Money Transfer “Sends” and “Receives”

For money transfer “Sends” and/or “Receives” of \$1,000 or more, you must obtain and record all of the information requested on both the front and back of the Send/Receive form.

You should maintain the following client information for all “Send” and “Receive” Transactions of \$1,000 or more:

- Name;
- Physical Address;
- Phone Number (if the client doesn't have a phone number, please reflect that on the form);
- Date of Birth;
- Identification Document;
- Specific Occupation;
- Sender or Receiver Name;
- Reference Number and Date of Transaction;
- Amount and Currency of the Transaction; and
- Similar Third Party Details (if a client is acting on behalf of another person).

If your business prints transaction receipts rather than having the client fill out a Send/Receive form, you must obtain the client's signature on the transaction receipt. By completing the front and back of the Send/Receive Form and / or having the client sign the transaction receipt, you should have all of the information that you are required to obtain.

You must retain the physical documents for all money transfers of \$1,000 or more for five (5) years.



Third Party Transaction Requirements

If you know that your client is sending or receiving a transaction on behalf of someone else, then you must also obtain the similar information on that other person. Examples of this could be a relative of an elderly person conducting a receive transaction for the elderly person. In this example, you must collect and document identifying information for both the person conducting the transaction and the person that the money belongs to.

MoneyGram's Identification Requirements

Before completing any Send money transfer of \$1,000 or more, you must verify the client's identity by examining a valid, original piece of government issued photo identification that contains the person's name, address, such as a driver's licence, passport or Provincial/Territorial government-issued ID card.

- Health insurance cards with photo issued by Ontario, Manitoba and Prince Edward Island, should NEVER be accepted as identification as the law prohibits it.
- A Health card or drivers licence issued by Quebec can be accepted if the client provides it but you cannot request it for identification purposes.

For all Receive money transfers, regardless of amount, you must verify the client's identity. Test questions are permitted of money transfers up to \$999 if the beneficiary does not have acceptable photo identification. Identification details or the answer to the test question must be recorded for "Receive" amounts.

Maximum Aggregated Transactions

The maximum send amount per transaction is \$10,000. MoneyGram allows a client to sent no more than two maximum amount transactions per day, or \$20,000.

Under no circumstances are you permitted to send multiple transactions for a person or related persons totaling \$100,000 or more in any consecutive 24-hour period. Combined transactions of \$100,000 or more require you to determine and document if the sender and / or receiver is a politically exposed foreign person (PEP).



Question: How does an Agent verify the identity of a client?

An Agent must verify the identity of a client by viewing an original, valid identification document that contains the client's name and preferably photograph and address. Official documents that may be used to verify the client's identity include a driver's license, passport or other government issued photo identification. Although it is not necessary to verify other information obtained from the client, if you believe the information provided is false, do not complete the transaction.

Question: How long must Agents keep information on money transfers of \$1,000 or more?

Agents must keep all records required by the PCMLTFA for a period of five (5) years from the date of the transaction.

Question: How should required records be kept?

Records must be kept in such a way that they can be provided to FINTRAC within 30 days of a request to examine them. You can keep them in a machine-readable or electronic form as long as a paper copy can be readily produced. For records that are kept electronically, an electronic signature of the individual who must sign the record must be retained. Where a document contains an original signature, the original document must be retained.

Section V.

Transaction Reporting

Large Cash Transaction Report (LCTR)

The Large Cash Transaction Report (LCTR) must be filed with FINTRAC for each transaction where you receive cash from or on behalf of the same person that equals \$10,000 or more in any consecutive 24-hour period. This report must be filed within 15 days of the transaction. The \$10,000 amount includes both the face amounts of the transaction and the fees paid by the purchaser(s).

MoneyGram will file this report for you unless other arrangements have been made.

The LCTR Form and instructions are available on the FINTRAC website at: www.fintrac.gc.ca.

Necessary Information for the LCTR

Although MoneyGram files the LCTR for you, we need you to collect and record the client's information for us. The LCTR requires you to collect the following client information *before you complete the transaction*:

- Name, physical address and phone number;
- Valid, original identification (including the type, number and place of issuance);
- Date of birth; and
- Occupation (be specific and descriptive, for example, *information technology consultant* is much better than *consultant*).

If two or more people are conducting the transaction, you must obtain the same information for all parties *before you complete the transaction*.

Third Party Transaction

For every large cash transaction of \$10,000 or more within a 24-hour period, you have to take reasonable measures to determine whether the individual who gives you the cash is acting on behalf of a third person. If you determine that there is a third party, you have to keep a record of the third party's:

- Name;
- Address;
- Principal business or occupation; and
- Relationship with the person who gives you the cash.

If you do not know if there is a third party, but you have reasonable grounds to suspect that the individual is acting on behalf of a third party, you have to keep a record to indicate whether the transaction is being conducted on behalf of a third party. This record must also indicate details of why you suspect that the individual is acting on behalf of a third party.



Large Cash Transaction Recordkeeping

You must keep all Send/Receive forms and/or transaction receipts for every large cash transaction of \$10,000 or more within a 24-hour period for five (5) years.

Large International Electronic Funds Transfer Report

An Electronic Funds Transfer Report (EFT) must be filed with FINTRAC for each money transfer involving a large international EFT requested by (or on behalf of) the same person of \$10,000 or more. This report must be filed within five (5) days of the transfer. An EFT Report is required for:

- Single money transfers of \$10,000 or more sent to a destination outside Canada;
- Two (2) or more transfers that total \$10,000 or more in any 24 hour period sent to a destination outside Canada;
- Receipt of a money transfer from a destination outside Canada of \$10,000 or more; and
- Receipt of multiple money transfers totaling \$10,000 or more in any 24 hour period from a destination outside Canada.

Multiple money transfers must be treated as a single transaction if you have knowledge that they are requested by (or on behalf of) the same person and total \$10,000 or more during any 24 hour period.

MoneyGram will file this report for you unless other arrangements have been made.

The EFT Report and instructions are available on the FINTRAC website at: www.fintrac.gc.ca.

Necessary Information for EFT Reports

Although MoneyGram files EFT Reports for you, we need you to collect and record the client's information for us. An EFT Report requires you to collect the following client information *before you complete the transaction*:

- Name, address and phone number;
- Valid, original identification (including the type, number and place of issuance);
- Date of birth; and
- Occupation.

If two or more people are doing the transaction, you must obtain the same information for all parties before you complete the transaction.

EFT Report Recordkeeping

Keep all Send/Receive forms and/or transaction receipts for every large cross border transaction of \$10,000 or more within a 24-hour period for five (5) years.



Section VI.

Structuring

Many money launderers are familiar with the dollar thresholds that require recordkeeping and reporting. Therefore, in order to remain anonymous and avoid the detection of law enforcement officials, they will “structure” their transactions so that the recordkeeping or reporting requirements will not be triggered. Structuring is the act of breaking up a potentially large transaction into several smaller ones to avoid reporting or recordkeeping requirements.

It is illegal for you or your clients to structure transactions in order to avoid the recordkeeping or reporting requirements. For example, if a client sends a \$750 money transfer in the morning and another \$750 money transfer send transaction in the afternoon, he may be structuring his purchases in order to avoid the \$1,000 recordkeeping requirements.

Likewise, it is illegal for you or your employees to assist anyone in structuring transactions in order to avoid recordkeeping or reporting requirements. For example, you may not tell or even imply to a client that they can avoid providing information by conducting a smaller transaction. Some criminals may attempt to trick you or your employees into allowing them to structure transactions by splitting up their activity with several accomplices or by trying to “con” you with a hard luck story. You need to be on the lookout for structuring so that you prevent it from occurring.

Question: Are all multiple transactions considered structuring?

No. For example, a client sends two money transfers to separate receivers, one for \$900 and another for \$500. Each transfer is less than \$1,000, but the total transaction exceeds \$1,000. There was nothing suspicious about the transactions and you learn that the client is sending money to her children who are attending two different schools. You should record the appropriate information on the back of the Send form in order to fulfill the recordkeeping requirement and to show that there was no attempt to structure the transactions.

Section VII.

Suspicious Activity

“Suspicious Activity” is a difficult concept to define, because it can vary from one transaction to another based upon on all of the circumstances surrounding the transaction or group of transactions. For example, transactions by one client may be normal, because of your knowledge of that client, while similar transactions by another client may be suspicious. Many factors are involved in determining whether the transactions are suspicious, including the amount, the locations of your business, comments made by your client, the client’s behavior, etc. That is why it is important for you to read this Guide in order to help you detect suspicious activity and structured transactions.

Reporting Suspicious Activity

MoneyGram must report suspicious transactions and attempted transactions to FINTRAC within 30 days of the suspicious event using a Suspicious Transaction Report (STR). To help us report suspicious activity and complete the STR, we need you to report suspicious transactions and suspicious attempted transactions on the following Canadian Activity Report (CAR).

MoneyGram
Canada Activity Report

Only agents in Canada should use this form.
Agents in the United States MUST report suspicious activity on a SAR-MSB.

If you have questions about this form or reporting suspicious activity, please call the MoneyGram Compliance Team at 1-800-642-8050 ext. 4500.

Use this form to document suspicious, unusual or unexplained customer activity within 5 days of the occurrence.

- Do NOT tell your customer you are completing this report. It is illegal to tell someone you think their activity is suspicious.
- Please print legibly.

This report must be faxed to 720-568-8640 the same day it is completed.

Today's Date: _____ Correction / amendment to a previous report: No Yes, date: _____

Business Name: _____ Agent Number: _____

Your Name: _____ Position / Title: _____

Business Address: _____ Phone Number: _____

City: _____ Province: _____ Postal Code: _____

Transaction or Attempted Transaction Details
Please check all that apply and provide details:

Date(s) Suspicious Activity Occurred: _____ Time Suspicious Activity Occurred: _____

Transaction funds: Cash Cheque Money Order EFT

Attempted Money Transfer Send(s) and/or Receive(s)

Completed Money Transfer Send(s) Reference Number(s): _____

Completed Money Transfer Receive(s) Reference Number(s): _____

Total Amount of Reported Activity or attempted activity: \$ _____ CAD USD

Customer Information
Please provide any / all of the following information. If information is unavailable, please leave the line blank.

Surname: _____ Given Name: _____ Other / Initial: _____

Street Address: _____

City: _____ Province / State: _____ Country: _____

Postal Code: _____ Country of Residence: _____ Country of citizenship: _____

Home Phone: _____

CONFIDENTIAL - FOR COMPLIANCE USE ONLY

Customer Details
Please provide any / all of the following information. If information is unavailable, please leave the line blank.

Customer Identifier: Birth Certificate Driver's License Passport Provincial Health Card
 Permanent Resident Card Other: _____

ID Number: _____ Issuing Province / State: _____ Issuing Country: _____

Date of Birth: _____

Occupation: _____ Employer: _____

Other Identifying Information: _____

Third Party Transaction Information, if applicable
Please provide any / all of the following information. If information is unavailable, please leave the line blank.

Transaction Conducted on Behalf of Another Party: No Yes

Business, Name of Business: _____

Type of Business: _____

Street Address: _____

City: _____ Province / State: _____ Country: _____

Business Phone: _____ Incorporation Number: _____

Individual, Surname: _____ Given Name: _____ Other / Initial: _____

Street Address: _____

City: _____ Province / State: _____ Country: _____

Postal Code: _____ Country of Residence: _____ Country of citizenship: _____

Home Phone: _____

Customer Identifier: Birth Certificate Driver's License Passport Provincial Health Card
 Permanent Resident Card Other: _____

ID Number: _____ Issuing Province / State: _____ Issuing Country: _____

Date of Birth: _____

Occupation: _____ Employer: _____

CONFIDENTIAL - FOR COMPLIANCE USE ONLY
MoneyGram and the Globe are TM/MC of MoneyGram. © 2008 MoneyGram. All rights reserved.

Customer Details
Please provide any / all of the following information. If information is unavailable, please leave the line blank.

Customer Identifier: Birth Certificate Driver's License Passport Provincial Health Card
 Permanent Resident Card Other: _____

ID Number: _____ Issuing Province / State: _____ Issuing Country: _____

Date of Birth: _____

Occupation: _____ Employer: _____

Other Identifying Information: _____

Third Party Transaction Information, if applicable
Please provide any / all of the following information. If information is unavailable, please leave the line blank.

Transaction Conducted on Behalf of Another Party: No Yes

Business, Name of Business: _____

Type of Business: _____

Street Address: _____

City: _____ Province / State: _____ Country: _____

Business Phone: _____ Incorporation Number: _____

Individual, Surname: _____ Given Name: _____ Other / Initial: _____

Street Address: _____

City: _____ Province / State: _____ Country: _____

Postal Code: _____ Country of Residence: _____ Country of citizenship: _____

Home Phone: _____

Customer Identifier: Birth Certificate Driver's License Passport Provincial Health Card
 Permanent Resident Card Other: _____

ID Number: _____ Issuing Province / State: _____ Issuing Country: _____


Date of Birth: _____

Occupation: _____ Employer: _____

CONFIDENTIAL - FOR COMPLIANCE USE ONLY
MoneyGram and the Globe are TM/MC of MoneyGram. © 2008 MoneyGram. All rights reserved.

You must file a CAR

with the MoneyGram



Compliance Department whenever a transaction is attempted or completed and you suspect or have reason to suspect that:

- The transaction is related to the commission of a money laundering offence; or
- The transaction is related to the commission of a terrorist financing activity offence.

Examples of Suspicious Activity

The following list provides examples of potentially suspicious activity that should raise concern and may result in the filing of a CAR:

- A client processes multiple cash transactions in a single day.
- A client appears to be structuring transactions in an attempt to avoid a PCMLTFA record-keeping or reporting requirement.
- An individual provides phony or expired identification.
- Two or more individuals, who are obviously together, split up to conduct separate transactions for under \$1,000, but which together add up to over \$1,000.
- An individual refuses to proceed with a transaction once he/she is informed a LCTR will have to be filed.
- A client asks an employee how to avoid reporting or record-keeping requirements.
- An individual attempts to threaten, or bribe an employee.
- Several clients complete transfers to the same recipient in a single day, and there is no apparent business reason for such transfers.
- The same person sends one or more MoneyGram electronic funds transfers several times a day, but never sends more than \$1,000 during any visit.
- A client knows very little about the address and / or contact details for a payee or the client is reluctant about providing this information.
- A client conducts transactions with parties in locations that are unusual for the client.
- A client conducts transactions in high dollar amounts or the client's activity over a period of time is excessive when compared to other clients.
- A client processes multiple cash transactions in a single day that total more than \$10,000 in an attempt to avoid the LCTR requirement.

***The only opportunity to verify client information
and identify suspicious activity is at the point of sale.
This can only be done with a knowledgeable, well-trained staff.***



Never Tell Your Client that You are Filing the STR or CAR

It is illegal for you to tell your client that you are suspicious of his / her activity and the STR may be filed. If MoneyGram believes that some of your clients may be misusing our money transfers, our compliance staff may contact you as part of an investigation. You must not tell your client about such an inquiry.

FINTRAC Notifications

We may report any suspicious transactions involving our products or services that we identify to FINTRAC or other government law enforcement officials. You must notify us immediately if FINTRAC or other government law enforcement officials contact you about a transaction involving our money transfers or other products or services we offer. We recommend that you also notify your lawyer of any such contacts.

Filing a STR

The STR must be filed within 30 days of the suspicious event. The STR form must be filed electronically if you have the technical capability to do so. Otherwise, the STR may be sent in paper format to FINTRAC. Forms are available on the FINTRAC website at: www.fintrac.gc.ca or by calling 1-866-346-8722.

Filing the CAR with MoneyGram International

To help us file the STR within the required time frame, we ask that you complete and send CAR forms to MoneyGram within 5 days of the suspicious event.

The CAR form should be completed legibly and faxed to MoneyGram within 5 days of the suspicious activity. Please call MoneyGram at 1-800-642-8050 ext. 4900 for additional information.



Question: What is the difference between the STR and the CAR?

MoneyGram is required to file the Suspicious Transaction Report on any suspicious transaction that was conducted or attempted with 30 days of the suspicious event. The Canadian Activity Report (CAR) is the report MoneyGram needs agents to complete to notify us when suspicious activity has occurred or has been attempted.

Question: What is the timing for filing the CAR?

MoneyGram must file the STR no later than 30 days after the attempted transaction or transaction took place, so we ask that you send us the CAR within 5 days of the suspicious event.

Question: Should I file supporting documentation with the CAR?

No. You should keep a copy of the CAR and all original supporting documentation or business record equivalent (including copies of instruments, receipts, photographs, surveillance audio or video tapes, etc.) for 5 years from the date of filing the CAR. All supporting documentation must be made available to appropriate authorities upon request.

Question: Can I file the STR directly to FINTRAC instead of filling out the CAR?

Yes, absolutely! MoneyGram is ultimately responsible for ensuring that the STR is filed, but all MoneyGram agents are welcome to file directly with FINTRAC. STR forms must be sent electronically if you have the technical capability to do so. If not, a paper format may be submitted to FINTRAC. If the paper format is used, the STR should be typed or legibly handwritten in black ink and CAPITAL LETTERS.

Question: Who should I call if I have other questions about suspicious activity or filing a CAR?

Please call the MoneyGram Anti-Money Laundering Compliance Team at 1-800-926-9400 x 4899 for additional information, if you have any other questions about suspicious activity or if you should file a CAR.



Section VIII.

Anti-Terrorist / Sanctions Legislation

Terrorist Group Property Report

A terrorist or terrorist group includes anyone that has as one of their purposes or activities, facilitated or carried out any terrorist activity. A terrorist also includes anyone on a list published under the *Criminal Code*. 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): www.osfi-bsif.gc.ca.

Under the *Criminal Code*, every person is required to disclose to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) the following:

- The existence of property in their possession or control that they know is owned or controlled by or on behalf of a terrorist group; and
- Information about a transaction or proposed transaction that you know was conducted by a terrorist group or on behalf of a terrorist group.

The RCMP can be contacted at:

- RCMP Financial Intelligence Task Force unclassified fax: (613) 993-9474; or
- RCMP Information Line: 1-888-349-9963

The CSIS can be contacted at:

- CSIS Security Screening Branch, Project Leader Government Operations, unclassified fax: (613) 842-1902.

Under the PCMLTFA, whenever a disclosure is made under the *Criminal Code*, a report must also be filed with FINTRAC. The form to be used for reporting to FINTRAC is a Terrorist Group Property Report.

Filing a Terrorist Group Property Report

You must file a Terrorist Group Property Report with FINTRAC, without delay. Unlike other reports to FINTRAC, the Terrorist Group Property Report is only available in paper format. Forms are available on the FINTRAC website at: www.fintrac.gc.ca or by calling 1-866-346-8722.

Terrorist Group Property Report Recordkeeping

You must keep a copy of the report and all supporting documentation for at least five (5) years.

The FINTRAC website provides information regarding the anti-terrorism measures contained in both the PCTFA and the *Criminal Code* at: www.fintrac.gc.ca.



United Nations Act

The *United Nations Act* enables the Canadian government to give effect to decisions made by the United Nations Security Council (UNSC). Currently, there are a number of country-specific sanctions under this Act.

Suppression of Terrorism Regulations

In addition, the *Suppression of Terrorism Regulations* were recently introduced to address anti-terrorist measures passed by the UNSC. Generally, such Regulations prohibit any person from providing or collecting any funds or dealing with a “Listed Person”. A “Listed Person” is defined to include persons established by the UNSC and any person listed on the schedule to the Regulations. The *Suppression of Terrorism Regulations* also require disclosure to the RCMP and CSIS of

- (a) The existence of property in their possession or control that they have reason to believe is owned or controlled by a Listed Person, or
- (b) Information about a transaction or proposed transaction in respect of property referred to in (a).

The Department of Foreign Affairs and International Trade provides information regarding various Canadian economic sanctions, including the *Suppression of Terrorism Regulations*, and links to available lists of individuals and entities subject to such sanctions at:

www.dfait-maeci.gc.ca/trade/sanctions-en.asp. The Department of Foreign Affairs and International Trade provides information regarding various Canadian economic sanctions, including the *Suppression of Terrorism Regulations* and links to available lists of individuals and entities subject to such sanctions at:
www.dfait-maeci.gc.ca/trade/sanctions-en.asp.

Special Economic Measures Act

Absent a resolution from the UNSC, authority exists under the *Special Economic Measures Act* to impose sanctions by means of orders or regulations. Currently, there are no regulations under this statute.

For additional information regarding anti-money laundering laws in Canada, refer to the FINTRAC web-site: www.fintrac.gc.ca. The FINTRAC website also provides information regarding the anti-terrorism measures contained in the PCMLTFA and the *Criminal Code* at: www.fintrac.gc.ca.



Section IX.

Civil and Criminal Penalties

The government requires strict compliance with all laws and regulations. The penalties for violating the PCMLTFA, the Criminal Code, the United Nations Act, or any of the regulations made under such statutes include fines and possible prison terms. Under certain circumstances, businesses can be held criminally liable for the acts of their employees; it is important for your employees to be trained in these matters and for your business to have a system in place to ensure employees' compliance with the laws and regulations. If you or your employees do not comply, you may be subject to large fines and/or imprisonment.

Directors or officers of an entity that have committed an offence could also be subject to penalties for the entity's non-compliance. MoneyGram may immediately cancel the contract of any agent who knowingly or negligently fails to comply with the laws and regulations.

Non-compliance just isn't worth the risk.

Keep this Guide

As this Guide has made clear, it is extremely important that you and your employees thoroughly understand the requirements of anti-money laundering laws and regulations. We have provided this Guide to help you in this important task. Make sure that all of your employees read and understand this Guide.

You may order more copies of the Guide through your Sales Representative. If you have questions about the provision of the laws and regulations, consult your lawyer, as we cannot give you legal advice. The penalties for non-compliance are severe, and the government will not readily accept ignorance or confusion about the regulations as an excuse.