

GUIDE TO COMPLY WITH CANADA'S ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING (AML/ATF) LEGISLATION

MARCH 2022

Guide to Comply with Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Legislation

MARCH 2022

DISCLAIMER

This publication provides general information only and does not constitute authoritative guidance. For such guidance, please refer to the relevant legislation and regulations. CPA Canada does not accept any responsibility or liability that may occur directly or indirectly as a consequence of the use, application or reliance on this material. An appropriately qualified professional should be consulted for advice in the application of the relevant legislation and regulations, as required.

ABOUT CPA CANADA

Chartered Professional Accountants of Canada (CPA Canada) works collaboratively with the provincial, territorial and Bermudian CPA bodies, as it represents the Canadian accounting profession, both nationally and internationally. This collaboration allows the Canadian profession to champion best practices that benefit business and society, as well as prepare its members for an ever-evolving operating environment featuring unprecedented change. Representing more than 220,000 members, CPA Canada is one of the largest national accounting bodies worldwide. cpacanada.ca

© 2022 Chartered Professional Accountants of Canada

All rights reserved. This publication is protected by copyright and written permission is required to reproduce, store in a retrieval system or transmit in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise).

For information regarding permission, please contact permissions@cpacanada.ca

Foreword

Chartered Professional Accountants of Canada (CPA Canada) has commissioned this *Guide to Comply with Canada's AML/ATF Legislation*¹ to help CPA Canada members and accounting firms deal with changes in AML/ATF regulatory requirements since this guide was last published in 2014.

Accountants and accounting firms (as those terms are defined by the AML/ATF legislation) are reporting entities under Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) that must comply with specific regulatory requirements when they engage in certain activities.

The regulator responsible for ensuring adherence to that legislation is the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC issues its own guidance to assist individuals and entities to comply with their obligations and it should be reviewed in conjunction with the information provided in this guide.

Non-compliance with the AML/ATF legislation by accountants and accounting firms creates a risk of administrative monetary penalties or even criminal sanctions. If a penalty is imposed, the name of the accountant and/or the accounting firm, the nature of the violation and the amount of the penalty will be made public, creating a reputational risk. Therefore, an effective AML/ATF compliance program that stays up to date with evolving legislation is key to mitigating these risks.

This publication aids accountants and accounting firms by addressing comprehensive topics including:

- international AML/ATF standards and the Canadian regime
- Canadian AML/ATF legislation and a Criminal Code amendment to the definition of money laundering

¹ In this guide, the expression AML/ATF legislation refers to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its related regulations.

- who and what activities fall within the AML/ATF obligations such as:
 - development of a compliance program
 - money laundering and terrorist financing risk assessment
 - what reports need to be submitted to FINTRAC
 - record keeping
 - know your client obligations
 - determination of beneficial ownership
 - ongoing monitoring of business relationships
 - measures when dealing with politically exposed persons, heads of international organizations, their families and close associates
 - AML/ATF and privacy obligations
- FINTRAC examinations

Chapters 2 to 5 have been designed to give accountants and accounting firms a general understanding of the international and domestic landscape for AML/ATF and the five key Canadian AML/ATF legislation obligations that must be met if required:

- implementing and maintaining a compliance program
- knowing your client
- keeping records
- reporting and ministerial directives and transaction prohibitions

Chapter 6 details how accountants and accounting firms may meet the obligation to implement and maintain a compliance program, while Chapters 23 and 24 cover in greater depth the obligations for knowing your client and verifying the identity of a person or entity.

Chapters 7 to 11, and Chapter 15 provide detailed, practical guidance covering nine scenarios that an accountant or accounting firm may encounter in connection with meeting the requirements imposed by the AML/ATF legislation. They contain explanations of what to do, if applicable when:

1. receiving funds of less than \$3,000
2. receiving funds of \$3,000 or more
3. reporting a suspicious transaction or attempted transaction
4. reporting receiving \$10,000 or more in cash
5. reporting receiving \$10,000 or more in virtual currency
6. receiving \$100,000 or more in cash from a politically exposed person (PEP), a head of an international organization (HIO), their family members or close associates
7. receiving \$100,000 or more in virtual currency from a PEP, HIO, their family members or close associates
8. reporting terrorist property
9. dealing with PEP, a HIO, their family members or close associates

Throughout the guide there are questionnaires and other tools to help accountants and accounting firms ask the right questions, and practical guidance on how to complete FINTRAC forms. Unless otherwise indicated, all references to funds or virtual currency are in Canadian denominations.

While every effort has been made to ensure that the information in this guide is clear, accurate and reflective of the AML/ATF legislation as of June 1st, 2021 and publicly available FINTRAC guidance documents,² this guide should not be viewed as authoritative. Accountants and accounting firms must continue to stay up to date with the AML/ATF legislation itself, along with related guidance, and policy interpretation changes going forward.

CPA Canada would like to thank those who assisted in the development and updating of this guide.

² A listing of links to FINTRAC guidance relevant to accountants and accounting firms is included in Chapter 17 Appendix C - Links to FINTRAC guidance.

Table of Contents

Please note that a number of important definitions and acronyms can be found in chapter 3.5 of this guide.

Foreword	v
CHAPTER 1	1
Purpose of the guide	1
CHAPTER 2	3
Money laundering and terrorist financing	3
2.1 A global fight	3
2.2 International standards	4
2.3 Canada's AML/ATF legislation	4
2.3.1 ML threshold in the Criminal Code	5
2.3.2 The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and related regulations	6
CHAPTER 3	7
Determining if the obligations are applicable	7
3.1 Definition of accountant and accounting firm	7
3.2 Definition of triggering activities	8
3.2.1 Giving instructions versus giving advice	10
3.2.2 Specific exemptions and considerations	10
3.2.2.1 Employment relationship	11
3.2.2.2 Assurance related activities	11
3.2.2.3 Trustee in bankruptcy services	11
3.2.2.4 Implications of organizational structure	12
3.2.2.5 A note on voluntary triggering activities	13
3.2.2.6 A note on client fees	13

3.3	Questionnaires to assist in determining applicability	13
3.3.1	Do I have obligations as an accountant?	13
3.3.2	Do we have obligations as an accounting firm?	16
3.4	Determination of triggering activities	17
3.5	A few important definitions and acronyms	18
3.5.1	Definitions	18
3.5.2	Acronyms	26
CHAPTER 4		29
Engaged in triggering activities, now what?		29
4.1.	Implement and maintain a compliance program	29
4.2	Know your client	30
4.2.1	Verify the identity of a person and verify the identity of an entity	31
4.2.1.1	FINTRAC examination	33
4.2.2	Determining business relationships and ongoing monitoring	35
4.2.2.1	Business relationship	35
4.2.2.2	Ongoing monitoring	37
4.2.2.2.1	Ongoing monitoring records	39
4.2.2.2.2	FINTRAC examination	39
4.2.3	Beneficial ownership requirements	41
4.2.3.1	Reasonable measures to obtain beneficial ownership information and confirm its accuracy	43
4.2.3.2	Exceptions to beneficial ownership requirements	46
4.2.3.3	FINTRAC examination	47
4.2.4	Is a third-party giving instructions to your client?	48
4.2.4.1	FINTRAC examination	50
4.2.5	Business relationships with politically exposed persons (PEPs), their family members and close associates	50
4.2.5.1	FINTRAC examination	51
4.2.6	Have you assessed your client as high risk?	52
4.3	Keep records and copies of reports	54
4.3.1	Reasonable measures	55
4.3.2	FINTRAC examination	56
4.4	Submit reports to FINTRAC	57
4.4.1	FINTRAC examination	59

4.5	Ministerial directives and transaction limitations/prohibitions	61
4.5.1	Ministerial directives	62
4.5.2	Transaction limitations/prohibitions	63
4.5.3	FINTRAC advisories about financial transactions related to countries identified by the Financial Action Task force (FATF)	64
4.5.4	FINTRAC examination	64
4.6	Exceptions	66
4.6.1	Record keeping exceptions	66
4.6.2	Reporting exceptions	68
4.7	Table summarizing what to do in eight special events when engaged in triggering activities	68
CHAPTER 5		75
About money laundering and terrorist financing		75
5.1	Money laundering	75
5.1.1	Concealment within business structures	76
5.1.2	Misuse of legitimate businesses	76
5.1.3	Use of false identities, documents or straw men	76
5.1.4	Exploiting international jurisdictional issues	77
5.1.5	Use of anonymous asset types	77
5.2	Terrorist financing	77
5.3	Indicators of money laundering and terrorist financing	79
CHAPTER 6		81
Implement and maintain a compliance program		81
6.1	Appoint a compliance officer	83
6.1.1	Sample role description of a compliance officer	84
6.1.2	FINTRAC examination	84
6.2	Develop and apply written compliance policies and procedures	86
6.2.1	General policies	87
6.2.1.1	Compliance program	87
6.2.1.2	Know your client	88
6.2.1.2.1	Verification of identity and verification of existence	88
6.2.1.2.2	Third-party determination	89
6.2.1.2.3	Beneficial ownership	89

6.2.1.2.4	Politically exposed persons, heads of international organizations, family members and close associates	90
6.2.1.3	Business relationships and ongoing monitoring	90
6.2.1.4	Record-keeping	90
6.2.1.5	Enhanced measures for high-risk clients	91
6.2.1.6	Transaction reporting	91
6.2.1.7	Ministerial directives and transaction limitations/prohibitions	92
6.2.2	Sample list of policies and procedures headings	92
6.2.3	FINTRAC examination	94
6.3	Assess and document the risk of ML/TF	95
6.3.1	Accountants' and accounting firms' risk of ML/TF	95
6.3.2	Requirement for a risk assessment	95
6.3.3	Risk assessment process	97
6.3.3.1	Risk assessment	98
6.3.3.1.1	Clients and business relationships	99
6.3.3.1.2	Products and delivery channels	99
6.3.3.1.3	Geographic location of the activities	99
6.3.3.1.4	New developments and impact of new technologies	100
6.3.3.1.5	Any other relevant factor	100
6.3.4	Risk mitigation	100
6.3.5	Ongoing monitoring of triggering activity business relationships	101
6.3.5.1	Defining the purpose and intended nature of a business relationship	102
6.3.5.2	Ongoing monitoring: Detecting suspicious transactions and assessing the consistency of transactions with client knowledge and risk	102
6.3.5.3	Ongoing monitoring: Keeping client identification information up to date	103
6.3.5.4	Ongoing monitoring: Reassessing client risk levels	103
6.3.5.5	When does ongoing monitoring end?	103
6.3.6	Enhanced measures	104
6.3.6.1	When does the requirement for enhanced monitoring end?	107
6.3.7	FINTRAC examination	107
6.4	Ongoing training program	109
6.4.1	FINTRAC examination	110

6.5	Instituting and documenting a training plan and delivering compliance training	111
6.5.1	Training topics and material	111
6.5.2	Training methods for delivery	112
6.5.3	Training frequency	113
6.5.4	Sample training plan	113
6.6	Review and test the effectiveness of your compliance program	114
6.6.1	Requirement for instituting and documenting of a plan for the two-year effectiveness review	115
6.6.2	Evaluation methods	116
6.6.2.1	Additional elements you may consider testing during your review	116
6.6.3	Sample scope	118
6.6.4	FINTRAC examination	119
CHAPTER 7		121
Receiving funds of less than \$3,000? What to do.		121
7.1	Do you consider the activities to be high risk?	121
7.2	Do you have a business relationship with the client?	122
7.3	If you have a business relationship with the client, is the client a PEP, HIO, a family member or close associate (of foreign PEP only, in certain circumstances)?	124
CHAPTER 8		125
Receiving funds of \$3,000 or more? What to do.		125
8.1	Keep a receipt of funds record	126
8.1.1	General exceptions	127
8.1.2	Specific exceptions	127
8.2	Verify the identity of the client and keep a record	129
8.2.1	Verifying the identity of persons	129
8.2.1.1	Keeping a record of verification of the identity of a person	130
8.2.2	Verifying the identity of an entity	131
8.2.2.1	Confirmation of existence method for a corporation	131
8.2.2.2	Confirmation of existence method for an entity other than a corporation	131
8.2.2.3	Reliance method	132
8.2.2.4	Record keeping requirements	133
8.2.2.5	Exceptions	133

8.3	Keep a business relationship and ongoing business relationship monitoring record (if applicable)	135
-----	--	-----

8.4	Keep a record of beneficial ownership and reasonable measures (if applicable)	136
-----	---	-----

CHAPTER 9 **141**

Report a suspicious transaction or attempted transaction **141**

9.1	What is a suspicious transaction report (STR)?	141
-----	--	-----

9.1.1	TPR vs STR	143
-------	------------	-----

9.2	Establish reasonable grounds for suspicion	145
-----	--	-----

9.3	Verification of client identity and no tipping off	150
-----	--	-----

9.4	Complete the STR	150
-----	------------------	-----

9.5	Record keeping	151
-----	----------------	-----

9.6	Exceptions	151
-----	------------	-----

9.7	FINTRAC examination	152
-----	---------------------	-----

CHAPTER 10 **153**

Report receiving \$10,000 or more in cash or in virtual currency **153**

10.1	The 24-hour rule	154
------	------------------	-----

10.1.1	Aggregation of transactions under the 24-hour rule	155
--------	--	-----

10.1.2	Application of the 24-hour rule to LCTRs and LVCTRs	155
--------	---	-----

10.2	Receiving funds of \$10,000 or more in cash	156
------	---	-----

10.2.1	Exceptions for LCT record keeping and LCT reports	156
--------	---	-----

10.3	Receiving \$10,000 or more in virtual currency	157
------	--	-----

10.3.1	Exceptions for LVCT record keeping and LVCT reporting	158
--------	---	-----

10.3.2	Examples applied to LVCTRs and the 24-hour rule	158
--------	---	-----

10.4	General exceptions	160
------	--------------------	-----

10.5	Verifying the identity of clients	160
------	-----------------------------------	-----

10.6	Keep records	161
------	--------------	-----

10.7	What is a large virtual currency transaction record?	164
10.7.1	Exception for large virtual currency transaction record	166
10.8	What is a large cash transaction record?	166
10.8.1	Sample large cash transaction record	167
10.9	Receiving \$100,000 or more in cash or virtual currency	168
10.9.1	What are the reasonable measures you must take to determine if the person is a politically exposed person, a head of an international organization, their family member or a close associate?	170
10.9.2	If I have made such a determination, now what?	171
10.9.2.1	Receipt of \$100,000 In cash or virtual currency from a politically exposed foreign person, their family member or a close associate	171
10.9.2.2	Receipt of \$100,000 in cash or virtual currency from a politically exposed domestic person, head of an international organization or family member or close associate	173
10.9.3	Exceptions	175
CHAPTER 11		177
Reporting terrorist property		177
11.1	Knowledge or belief of terrorist property	178
11.2	Definitions	178
11.3	Requirements	180
11.3.1	Knowing about a terrorist or a terrorist group	181
11.3.2	Believing that property is owned or controlled by or on behalf of a listed person	181
11.3.3	Suspicion that property is owned or controlled by or on behalf of a listed person	181
11.3.3.1	Suspicious transaction report	182
11.4	Lists/Schedule of terrorists, terrorist groups, and listed persons	182
11.5	Filing a terrorist property report	183
11.6	Keeping a record	184
11.7	Advising the RCMP and CSIS	184

CHAPTER 12	185
AML/ATF and privacy obligations	185
12.1 Summary of “know your client” requirements	186
12.2 Where AML/ATF and privacy get complicated	186
12.3 What does the AML/ATF legislation say about enhanced measures?	186
12.4 What is required for enhanced measures?	187
12.5 What information should be documented?	187
CHAPTER 13	189
Interactions with other reporting entities	189
CHAPTER 14	191
Sanctions	191
14.1 Administrative monetary penalties (AMPs)	191
14.1.1 Categories of violations	192
14.1.2 AMP process	193
14.2 Voluntary self-declaration of non-compliance	195
14.2.1 What FINTRAC’s assessment manual indicates on voluntary self-declarations of non-compliance	196
14.3 Offences	196
CHAPTER 15	199
Appendix A – Summary table of requirements when dealing with business relationships and a PEFP, PEDP, HIO, their family members or close associates	199
15.1 Definitions	201
15.2 Requirements when entering into a business relationship	203
15.3 Requirement to conduct periodic monitoring of your business relationships	205
15.4 Requirements when you detect a fact that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is axPEFP, a family member, or close associate of a PEFP	207

CHAPTER 16	209
Appendix B – Canada’s AML/ATF regime	209
16.1 Players	209
16.2 FINTRAC’s roles	210
16.3 FINTRAC assistance	211
16.3.1 Guidance	211
16.3.2 Interpretation notices	211
16.3.3 Policy interpretations	211
16.3.4 Other FINTRAC publications and services	212
16.4 FINTRAC examinations	213
16.4.1 FINTRAC’s powers	213
16.4.2 FINTRAC’s assessment manual	213
16.4.3 Examination phases	214
16.4.4 How to prepare for an examination	215
16.4.5 What to expect	216
16.4.6 Follow up	217
16.4.7 Compliance assessment report	218
CHAPTER 17	219
Appendix C – Links to FINTRAC guidance	219
CHAPTER 18	223
Appendix D – FINTRAC Interpretation Notice No. 2	223
CHAPTER 19	225
Appendix E – FINTRAC Interpretation Notice No. 7	225
CHAPTER 20	229
Appendix F – Relevant FINTRAC policy interpretations	229
20.1 Policy Interpretation PI No. 6171 answered on 2014-07-02: Clarification on record keeping retention	229
20.2 Policy Interpretation PI No. 6303 answered on 2015-04-28: On accounting sector questions	231
20.3 Policy Interpretation PI No. 4542 answered on 2009-03-09: On exchange rates - Bank of Canada	236

20.4	Policy Interpretation PI No. 6409 answered on 2016-03-30: On the existence of incorporation and ascertaining identity of clients	237
20.5	Policy Interpretation PI Number: PI-4606 modified on 2020-09-25: On length of being a PEP and maintaining records	240
20.6	Policy Interpretation PI Number: PI-11075 Date answered: 2020-12-15: On PEP – source of cash or funds	241
20.7	Policy Interpretation PI Number: PI-11073 Date answered: 2020-12-09: PEP – Members of the same board	243
20.8	Policy Interpretation PI Number: PI-11067 Date answered: 2020-11-26: Accountants – When are there requirements?	245
	CHAPTER 21	249
	Appendix G – Suspicious transaction report form	249
21.1	STR form, FINTRAC	249
21.2	STR instructions	249
21.2.1	How to submit STRs	251
21.2.2	Review and validation of reports by FINTRAC	252
21.2.3	Completing the STR form	254
21.2.4	Field completion instructions	258
	CHAPTER 22	269
	Appendix H – Sample receipt of funds record and instructions	269
	CHAPTER 23	273
	Appendix I – Verifying the identity of a person	273
23.1	Requirement	273
23.2	Methods of verifying the identity	274
23.3	Government-issued photo identification method	275
23.3.1	Use of the government-issued photo identification method if a person is not physically present	276
23.3.2	Record keeping requirements for the government-issued photo identification method	277

23.3.3	Sample record when using the government-issued photo identification method	277
23.3.4	Examples of acceptable photo identification documents	278
23.4	Credit file method	279
23.4.1	Record keeping requirements for the credit file method	281
23.4.2	Sample record when referring to information in a client's credit file	282
23.5	Dual-process method	282
23.5.1	What is a reliable source of information?	284
23.5.2	How to use a credit file under the dual-process method to verify the identity of an individual	285
23.5.3	Record keeping requirements for the dual-process method	285
23.5.4	Sample record when referring to information using the dual method	286
23.5.5	Examples of reliable sources of information for the dual-process method	288
23.6	Reliance method	290
23.6.1	Record keeping requirements for the reliance method	291
23.7	Summary of the methods to identify persons and associated record keeping obligations	292
23.8	You may also rely on an agent or mandatary to verify the identity of a person on your behalf	293
23.8.1	Examples of acceptable/not acceptable use of an agent or mandatary	295
23.8.2	Record keeping when relying on an agent or mandatary	296
23.9	Identifying a person less than 12 years old and a person less than 16 years old	297
23.10	Exceptions to the verification of the identity of a person	298
	CHAPTER 24	303
	Appendix J - Verifying the identity of an entity	303
24.1	Confirmation of existence method	303
24.1.1	Corporation	303
24.1.2	Other than a corporation	304
24.1.3	Record keeping requirements when verifying the identity of a corporation or other entity	304

24.2	Reliance method	305
24.2.1	Corporation or entity other than a corporation	305
24.3	Summary of methods to identify an entity and associated record keeping obligations	306
24.4	Exceptions to record keeping for the verification of identity of an entity	307
CHAPTER 25		309
Appendix K – Obtaining and recording beneficial ownership information		309
25.1.	Beneficial ownership information for a corporation	310
25.2	Beneficial ownership information for a widely held or publicly traded trust	310
25.3	Beneficial ownership information for a trust	310
25.4	Beneficial ownership information for an entity other than a corporation or trust	310
25.5	Beneficial ownership for a not-for-profit organization	311
25.6	Record keeping of beneficial ownership information	311
25.7	Sample – Record of beneficial ownership	313
CHAPTER 26		315
Appendix L – Business relationship and ongoing monitoring		315
26.1	Record keeping	316
26.1.2	Sample – Record of business relationship information	317
CHAPTER 27		319
Appendix M – Large cash transaction report form		319
27.1	LCTR form, FINTRAC	319
27.2	Completion of the LCTR form	319

CHAPTER 28	321
Appendix N – Large virtual currency transaction report form	321
28.1 LVCTR form, FINTRAC	321
28.2 Field instructions to complete a large virtual currency transaction report	321
CHAPTER 29	323
Appendix O – Terrorist property report form	323
29.1 TPR form, FINTRAC	323
CHAPTER 30	325
Appendix P – Money laundering and terrorist financing indicators – Accountants	325
CHAPTER 31	337
Appendix Q – Indicators of ML/TF related to virtual currencies	337
CHAPTER 32	341
Appendix R – Third-party determination record when receiving \$10,000 or more in cash or virtual currency	341
32.1 Requirement	341
32.2 Form – Third-party determination record	343
CHAPTER 33	345
Appendix S – Self-review checklist	345
Part A: Compliance framework evaluation	345
Part B: Operational compliance evaluation	349

CHAPTER 1

Purpose of the guide

Maintaining the reputation of the profession is a responsibility of all members.

With that in mind, this guide has three main purposes:

1. To help accountants and accounting firms determine if AML/ATF obligations are applicable to their activities.
2. To guide accountants and accounting firms to which AML/ATF legislation applies in the development of a program to comply with their obligations.
3. To educate accountants and accounting firms about the examination focus and enforcement methods by the supervisor, FINTRAC, and risks of non-compliance.

The guide itself does not constitute an AML/ATF program. As required by the AML/ATF legislation, each accountant and accounting firm involved in triggering activities must develop its own compliance program that includes six elements:

1. appointing a compliance officer
2. developing and implementing written compliance policies and procedures
3. conducting a risk assessment
4. developing and maintaining an ongoing training program
5. instituting and documenting a training plan
6. reviewing the effectiveness of the compliance program every two years

For more information on the requirement for a compliance program, please see Chapter 6.

There are many changes to the AML/ATF legislation that accountants and accounting firms must be aware of. This guide delivers insights into these changes and, particularly, the more commonly publicized ones, which include:

1. the requirement to report suspicious transactions changed from a 30-day time limit, to “as soon as practicable”

2. taking certain measures in their business relationships with politically exposed persons, heads of international organizations, their family members or close associates
3. collecting beneficial ownership information when they are required to verify the existence of a corporation or an entity other than a corporation
4. the 24-hour rule for aggregated transactions of \$10,000 or more in cash or in virtual currency
5. requirement to submit a Terrorist Property Report (TPR) “immediately” as opposed to “without delay”
6. amendments to the Criminal Code’s definition of money laundering have changed the threshold for that offence from “knowing or believing” one is dealing with the proceeds of crime to being “reckless” in being involved with them, elevating the risk of criminal offences for accountants and accounting firms when engaged in triggering activities

CHAPTER 2

Money laundering and terrorist financing

2.1 A global fight

There are no accurate statistics identifying the amount of money laundered worldwide. A commonly referenced estimate is two per cent to five per cent of global gross domestic product (GDP) which was produced by the International Monetary Fund (IMF) in 1998. This is consistent with more recent findings which signaled global money laundered reached USD \$1.6 trillion as of 2009.³ Not surprisingly, the metric appears to hold true even here in Canada. The 2019 British Columbia Expert Panel looking into money laundering estimated \$41.3 billion or 2.1 per cent of GDP was being laundered in Canada.⁴

There are many ways to launder money, but certain sectors of the economy are more vulnerable such as financial institutions. It has also long been recognized by the Financial Action Task Force (FATF) that the accounting profession is an at-risk profession. Several typology reports from the FATF starting in 1998 and subsequent years identified accountants and other professionals such as lawyers and notaries, as “gatekeepers” to the financial system⁵ as well as describing their vulnerabilities in other reports.⁶ As early as 2003, the FATF’s list of 40 recommendations included not only “gatekeepers” and financial institutions but a host of other designated non-financial businesses and professions (DNFBPs) as playing a central role in preventing ML/TF.

3 FATF, *Money Laundering*. “The United Nations Office on Drugs and Crime (UNODC) conducted a study to determine the magnitude of illicit funds generated by drug trafficking and organised crimes and to investigate to what extent these funds are laundered. The report estimates that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered.”

4 Expert Panel on Money Laundering in BC Real Estate, *Combating Money Laundering In BC Real Estate*, 2019

5 FATF, *Report on Money Laundering Typologies 2003-2004*, p. 24, 2004

6 FATF, *Guidance for A Risk-Based Approach, Accounting Profession*, June 2019

By 2002, Canada had already identified accountants as reporting entities and as a result of the September 11, 2001 terrorist attacks, updated the title of the legislation to *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.⁷

2.2 International standards

As the international standards-setting body in fighting ML/TF, the FATF, of which Canada was a founding member, has issued 40 recommendations (often referred to as standards) to be adapted to local context and implemented by its 38 members and countries belonging to nine regional FATF-Style Regional Bodies (FSRBs). Collectively, the membership agreeing to follow these standards encompasses almost every country on the globe, creating a comprehensive and international framework to fight ML/TF.

Two of the 40 recommendations specifically focus on accountants. The first⁸ requires that accountants meet customer due diligence and record keeping requirements in specific circumstances and generally similar activities in a Canadian context have been reflected in the Canadian AML/ATF legislation since 2002 (see Section 2.3 of this guide).

The second⁹ requires them to report suspicious transactions. Many of the FATF's other recommendations are applicable to accountants but also to other sectors, including the requirement to implement a "Compliance Program" (see Chapter 6 of this guide).

2.3 Canada's AML/ATF legislation

In this guide, the term AML/ATF legislation specifically refers to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its related regulations with which accountants and accounting firms are obligated to comply. However, a foremost part of the country's legislation is the Criminal Code that defines money laundering and terrorist financing.

7 Government of Canada, [Canada Gazette](#) Part II, Extra Vol. 136, No. 7, page 37, May 14, 2002

8 FATF, *International Standards on Combatting Money Laundering & the Financing of Terrorism and Proliferation, Recommendations*, recommendation 22, 2022

9 FATF, *International Standards on Combatting Money Laundering & the Financing of Terrorism and Proliferation, Recommendations*, recommendation 23, 2022

2.3.1 ML threshold in the Criminal Code

A 2019 amendment to the Criminal Code has redefined money laundering, lowering the threshold in establishing whether criminal charges can be laid, and a conviction obtained, for money laundering, using the concept of recklessness. Subsection 462.31(1) of the Criminal Code now defines money laundering as:

“Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that, **or being reckless as to whether**, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of (a) the commission in Canada of a designated offence; or (b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.”¹⁰
[Emphasis added]

No longer is “knowing or believing” the threshold in establishing whether money laundering has occurred, but the concept of “being reckless” has been legislated. This amendment may make it less challenging for law enforcement to charge and prosecutors to pursue a conviction.

To be “reckless” is to be aware that there is a danger that conduct could bring about the result prohibited by criminal law, and nevertheless persist, despite the risk. So, for example, it is now an offence for an individual aware of a risk that property may be proceeds of crime to carry out the prohibited activity. If an accountant is aware there is a risk proceeds may have been obtained or derived from money laundering and deals with the proceeds in any manner, the accountant could be charged with a criminal offence.

Recklessness involves knowledge of a danger or risk but proceeding with the course of conduct such that it creates a risk that the prohibited result will occur. Recklessness is a subjective concept, in that it is found in the attitude of someone who sees the risk and who takes a chance. However, a judge can draw an inference from evidence that it was evident property was from proceeds of crime and that someone was therefore reckless by proceeding with the conduct that led to the result prohibited by law.

¹⁰ Criminal Code subsection 462.31 (1)

All of this means that the stakes are now higher for accountants and accounting firms in ensuring that they know their clients, conduct proper risk assessments, and implement and maintain an effective compliance program to limit any risks of running afoul of the Criminal Code's money laundering provisions.

2.3.2 The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and related regulations

The PCMLTFA¹¹ and its five regulations constitute the legislative framework accountants and accounting firms must comply with when they are engaged in triggering activities. Of the five regulations, the following three are most relevant to accountants and accounting firms:

- The Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR),¹² which describe the obligations related to the reporting of suspicious and attempted transactions as well as the reporting of terrorists', terrorist group's and listed person's property.
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)¹³ that enact the bulk of the requirements to implement and maintain a compliance program (see Section 4.1), know your client (see Section 4.2), keep records (see Section 4.3), submit reports to FINTRAC (see Section 4.4) and comply with ministerial directives/transaction restrictions and prohibitions (see Section 4.5).
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (PCMLTFAMPR) that describe the list of violations to the PCMLTFA and its regulations, type and amount of penalties.¹⁴

The two other regulations are related to the registration of money services businesses¹⁵ and the reporting of the movement of cross-border currency and monetary instruments.¹⁶

11 Justice Laws Canada – [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Act](#), August 16, 2019

12 Justice Laws Canada – [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Suspicious Transactions Reporting Regulations](#)

13 Justice Laws Canada – [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations](#)

14 Justice Laws Canada – [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Administrative Monetary Penalties Regulations](#)

15 Justice Laws Canada – [Proceeds of Crime \(Money Laundering\) and Terrorist Financing Registration Regulations](#)

16 Justice Laws Canada – [Cross-border Currency and Monetary Instruments Reporting Regulations](#)

CHAPTER 3

Determining if the obligations are applicable

The AML/ATF legislation is applicable to accountants and accounting firms engaging in triggering activities (described in Section 3.2) under paragraph 5(j) of the PCMLTFA.¹⁷ Accountants and accounting firms have ongoing obligations to identify the performance of triggering activities and to perform all prescribed measures within specified timelines. As a practical matter, accounting firms are advised to perform annual training to make their organization aware of triggering activities in order that those in their firm are equipped to self-identify those circumstances. As a safeguard, accounting firms are advised to conduct an annual self-assessment to determine whether individuals in their organizations are involved in triggering activities, and to evaluate conformance of the related documentation to Canadian AML/ATF legislation. Questionnaires aimed at assisting that determination are included in Section 3.3.

3.1 Definition of accountant and accounting firm

The definition of an accountant has been changed to include the designation of a Chartered Professional Accountant. An “accountant” is now defined by the AML/ATF legislation as being a Chartered Accountant (CA), Certified General Accountant (CGA), a Certified Management Accountant (CMA) or, if applicable, a Chartered Professional Accountant (CPA).¹⁸

¹⁷ *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17)

¹⁸ PCMLTFR subsection 1(2).

An “accounting firm” is defined by the AML/ATF legislation as being an entity that is engaged in the business of providing accounting services¹⁹ to the public and has at least one partner, employee or administrator that is an accountant.²⁰

The definition of accountant does not require the professional to be engaged in providing professional accounting services to the public²¹ to be covered by the AML/ATF legislation, only that they are a designated accountant that performs, however infrequently, triggering activities.

An accountant is not subject to the AML/ATF legislation if they only perform triggering activities on behalf of their employer.²² However, if the accountant’s employer is an accounting firm, then the AML/ATF legislation does impose an obligation on both the accountant and accounting firm to report suspicious transactions and terrorist property.²³ An accountant performing any triggering activities for any client in addition to, or outside of their regular employment relationship would still be subject to the AML/ATF legislation, in respect of those outside activities.

3.2 Definition of triggering activities

Generally, triggering activities involve dealing with client assets on their behalf. Dealing with client assets might involve conducting transactions on their behalf or giving instructions to a party to conduct the transactions.²⁴ Exceptions and other considerations are explained in Section 3.2.2.

There are four categories of triggering activities which are listed below with illustrative examples. These examples do not represent an exhaustive list of all possible triggering activity scenarios.

19 Accounting services is not defined in the PCMLTFR. In Alberta, the Regulated Accounting Profession Act paragraph 1(ss) and (vv) defines “professional accounting practice” and “public accounting practice” to include the providing or offering to provide one or more of the following services to the public: (i) an assurance engagement; (ii) a compilation engagement; (iii) a specified auditing procedures engagement; (iv) accounting services; (v) forensic accounting, financial investigation or financial litigation support services; (vi) advice about or interpretation of taxation matters; (vii) preparation of a tax return or other statutory information filing, if prepared in conjunction with any service referred to in subclauses (i) to (vi).

20 PCMLTFR subsection 1(2)

21 See Section 20.2, FINTRAC Policy Interpretation PI-6303 answered on 2015/04/28.

22 PCMLTFR subsection 47(3)

23 FINTRAC, *Accountants*, July 12, 2021

24 The concept of giving instructions is explained in more detail in Section 3.2.1.

1. Receiving or paying funds or virtual currency^{25 26}
 - a. Your accounting firm performs bookkeeping services and has signing authority over the account of a not-for-profit organization client and pays invoices from that account on its behalf.
 - b. A client issues a cheque to you as a sole practitioner accountant in an amount equal to their income tax payable and your accounting fees. You then deposit the cheque and wire the income tax payable to the Canada Revenue Agency (CRA) from your account.
 - c. A client instructs their vendor to settle their invoice by remitting funds to your accounting firm and then asks that your firm issues a cheque for the difference between the value of the wire and your outstanding fees.
 - d. A client requests assistance in transferring funds from a sanctioned country into Canada, in respect of which an accountant arranges for Canadian accounts and wire transfers through intermediate countries.
2. Purchasing or selling real property, or immovables or business assets, or entities²⁷
 - a. The leader of the corporate finance group of your accounting firm travels to the U.S. to finalize the purchase of a business on behalf of their client.
 - b. Acting as the trustee for an estate, an accountant instructs a real estate broker to sell a piece of land owned by the estate.
3. Transferring funds, virtual currency or securities by any means²⁸
 - a. An accountant within your accounting firm has been engaged by the lawyer of a client without capacity to manage their investments and exercises discretionary authority to buy and sell securities on their behalf.
 - b. As part of a tax restructuring engagement, an accountant opens investment accounts in other countries on behalf of their clients and orders domestically held securities transferred there.
 - c. In connection with a corporate reorganization, an accountant documents and executes share transfers in a minute book on behalf of their client.

²⁵ Funds are defined in the PCMLTFR 1(2) as meaning “(a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.”

²⁶ Virtual currency is defined in the PCMLTFR 1(2) as meaning (a) a digital representation of value that can be used for payment or investment purposes, that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

²⁷ PCMLTFR paragraph 47(1)(b)

²⁸ PCMLTFR paragraph 47(1)(c)

4. Giving instructions in connection with any of the above (paragraphs 1,2 and 3 above).²⁹
 - a. Acting as the trustee for an estate, an accountant instructs a real estate broker to sell a piece of land owned by the estate.

3.2.1 Giving instructions versus giving advice

An interpretation notice³⁰ from FINTRAC distinguishes the concept of “giving instructions,” which would constitute a triggering activity in respect of any of the three categories noted above in section 3.2 (paragraphs 1,2 and 3), from “giving advice,” which would not constitute a triggering activity. Giving instructions is synonymous with “ordering” a specific transaction in this context (e.g., “Based on my client’s instructions, I request that you transfer \$600 from my client’s account 12345 to his other account 67890.”) Giving advice involves a recommendation to the client or their advisors rather than giving instructions to take action with respect to their assets (e.g., “For tax purposes, we recommend that you transfer your money into long-term investments.”)

3.2.2 Specific exemptions and considerations

Once it has been determined that you are an accountant or an accounting firm that engages in triggering activities, the AML/ATF legislation is applicable unless one of three exemptions apply:

1. In the case of an accountant who is acting in the capacity of an employee.³¹
2. In the case of an accountant or an accounting firm, where triggering activities are carried out in the course of an audit, a review or a compilation engagement within the meaning of the CPA Canada Handbook prepared and published by the Chartered Professional Accountants of Canada, as amended from time to time.³²
3. In the case of an accountant who is acting in the capacity of a person who either is authorized by law to carry on the business of – or to monitor the business or financial affairs of – an insolvent or bankrupt person or entity or is authorized to act under a security agreement.³³

29 PCMLTFR paragraph 47(1)(d)

30 See the Interpretation Notice No. 2 at Chapter 18 Appendix D – FINTRAC Interpretation Notice No. 2.

31 See FINTRAC Policy Interpretation PI-11067 at Section 20.8

32 PCMLTFR subsection 47(2)

33 PCMLTFR subsection 47(3)

Additionally, for risk and other legislative reasons, some accounting firms have incorporated a separate entity through which they conduct triggering activities. Those entities are typically subject to other provisions of the same AML/ATF legislation.

3.2.2.1 Employment relationship

As mentioned earlier, an accountant who performs triggering activities only for their employer is not subject to the AML/ATF legislation. Triggering activities performed by an accountant outside of their employment relationship would not be exempted by this provision. An accountant who both worked as full-time employee controller and maintained bookkeeping clients on whose behalf they transferred funds, would be covered by the AML/ATF legislation because of the latter activity, and only in respect of that latter activity.

3.2.2.2 Assurance related activities

The AML/ATF legislation holds that what would otherwise constitute triggering activities do not subject an accountant or an accounting firm to its obligations in cases where those activities are performed in respect of an “audit, a review or a compilation engagement within the meaning of the CPA Canada Handbook prepared and published by the Chartered Professional Accountants of Canada, as amended from time to time.”³⁴ Given the nature and standards governing those types of engagements, it is unlikely in any event that any triggering activities would be performed in connection with them.

3.2.2.3 Trustee in bankruptcy services

The PCMLTFR specifically states that an accountant who is acting in the capacity of an employee or of a person who either is authorized by law to carry on the business of – or to monitor the business or financial affairs of – an insolvent or bankrupt person or entity, or is authorized to act under a security agreement is not engaged in triggering activities, and therefore not subject to the PCMLTFA and its regulations in those circumstances.³⁵

FINTRAC also issued an interpretation notice³⁶ advising that accountants and accounting firms appointed by a court, or acting solely as a trustee in bankruptcy, are not considered to be acting on behalf of any other individual or entity, and therefore, are not engaged in triggering activities.

³⁴ PCMLTFR subsection 47(2)

³⁵ PCMLTFR subsection 47(3)

³⁶ See FINTRAC Interpretation Notice (IN) No. 7 at Chapter 19 Appendix E. Please note that IN No. 7 was issued on February 17, 2011, and that at the date of writing this guide, the definition of an accountant in IN No. 7 had not been adjusted to reflect the PCMLTFR change effective on June 1, 2021, to include Chartered Professional Accountants.

Additionally, FINTRAC advised in the notice that practices that only provide the services listed below are not considered to be “providing accounting services to the public,” and therefore would not be considered to be an accounting firm subject to the AML/ATF legislation:

1. As a receiver, pursuant to the provisions of a court order or by way of a private letter appointment pursuant to the terms of a security interest.
2. A trustee in bankruptcy.
3. As monitor under the provisions of the *Companies’ Creditors Arrangement Act* or any other proceeding that results in the dissolution or restructuring of an enterprise or individual and to which the firm, individual or insolvency practitioner serves as an officer of the court or agent to one or more creditors or the debtor.

Notwithstanding, a firm which provides any accounting services to the public outside of the scope of those three listed services will be deemed to be an accounting firm. An insolvency practice may, for instance, also perform restructuring and interim controller services outside of the context of an appointment which would bring their firm into the definition of an accounting firm. In that case, triggering activities performed by that practice, such as the sale of real property in the capacity of an interim controller, would subject them to the obligations of the prevailing AML/ATF legislation.

3.2.2.4 Implications of organizational structure

For risk management purposes and to comply with other legislation, it is common practice for accounting firms to incorporate separate entities – such as a corporate finance division – for activities that relate to purchasing or selling real property, business assets, entities or securities. If these entities do not offer accounting services to the public, then they would not be considered to be accounting firms and therefore not subject to the AML/ATF legislation on that basis. However, other obligations arise from the AML/ATF legislation for entities that are considered to be “securities dealers”³⁷ or real estate brokers. Firms that organize separate entities should comply with laws relevant to their activities and take care not to provide or offer accounting services to the public from those entities.

³⁷ The PCMLTFA subsection 5(g) defines “securities dealers” as being persons and entities authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity.

3.2.2.5 A note on voluntary triggering activities

Even if an accountant or accounting firm carries out triggering activities on a voluntary basis, they are subject to the requirements of the AML/ATF legislation.³⁸ Accountants and accounting firms are subject to the requirements of the AML/ATF legislation when engaged in triggering activities, regardless if fees are received or a formal letter of engagement to do so is obtained.


3.2.2.6 A note on client fees

Receiving payment for client fees does not in itself constitute a triggering activity as the funds are not received on behalf of a client – they are received on behalf of the firm itself. However, payments from clients where the amount is comprised of both fees and value for further payment to a third-party, such as the CRA, would be considered a triggering activity.



3.3 Questionnaires to assist in determining applicability

3.3.1 Do I have obligations as an accountant?


Table 1

Question	Response	Comment/Direction
1. Are you a professionally designated Accountant (CPA, CA, CMA, CGA)?	Yes	Designated professional accountants have responsibilities if they perform triggering activities. Proceed to question 2.
	No	Non-designated accountants do not have responsibilities to the AML/ATF legislation by virtue of being accountants. 

38 FINTRAC, [Accountants](#), July 12, 2021



Question	Response	Comment/Direction
2. Do you perform transactions that involve any of these triggering activities on behalf of a client (on a compensated or non-compensated basis)? a. receiving, paying funds or virtual currency b. purchasing or selling real property, or immovable or business assets, or entities c. transferring funds, virtual currency or securities by any means d. giving instructions in connection with any of the above	Yes	Performing triggering activities gives rise to obligations defined in the AML/ATF legislation, unless exceptions apply. Proceed to question 3.
	No	If no triggering activities are performed or offered, no obligations arise from the AML/ATF legislation by virtue of being an accountant. 
3. Are all triggering activities you perform or offer done so as part of your employment?	Yes	If all triggering activities are performed in the course of an employment relationship, the obligations defined by the AML/ATF legislation are not applicable. However, if the accountant's employer is an accounting firm, then the AML/ATF legislation does impose an obligation on both the accountant and accounting firm to report suspicious transactions and terrorist property. ³⁹ 
	No	If any one triggering activity is performed outside of an employment relationship, obligations set out in the AML/ATF legislation are applicable, unless other exemptions apply. Proceed to question 4.



39 FINTRAC, *Accountants*, July 12, 2021

Question	Response	Comment/Direction
<p>4. Are all triggering activities performed in connection with assurance engagements or as part of receiver/trustee/monitor in bankruptcy appointments?</p>	Yes	<p>If all triggering activities are performed in connection with assurance engagements or as part of receiver/trustee/monitor in bankruptcy appointments, obligations defined by the AML/ATF legislation are not applicable.</p> 
	No	<p>If any one triggering activity is conducted that is not performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by the AML/ATF legislation is applicable.</p> <p>LEGISLATION APPLICABLE</p>

3.3.2 Do we have obligations as an accounting firm?

Table 2

Question	Response	Comment/Direction
1. Does your firm provide accounting services to the public?	Yes	<p>An entity that provides any accounting services to the public may be considered an accounting firm if it has at least one partner, employee or administrator that is an accountant. Note that insolvency related engagements that involve appointments as: receiver, trustee in bankruptcy, or as monitor under the provisions of the <i>Companies' Creditors Arrangement Act</i> are not considered to constitute accounting services.</p> <p>Proceed to question 2.</p>
	No	<p>An entity that does not provide any accounting services to the public is not considered to be an accounting firm, and therefore would not have obligations pursuant to the AML/ATF legislation on that basis.</p> 
2. Is at least one of your entity's partners, employees, or administrators a professionally designated accountant (CPA, CA, CMA, CGA)?	Yes	<p>Any entity that offers accounting services to the public and has at least one designated professional accountant as a partner, employee or administrator is an accounting firm and would have responsibilities if they perform triggering activities.</p> <p>Proceed to question 3.</p>
	No	<p>Any entity that offers accounting services to the public, but has no designated professional accountants, partners, employees or administrators, is not considered to be an accounting firm, and therefore would not be subject to the AML/ATF legislation obligations on that basis.</p> 

Question	Response	Comment/Direction
3. Does your firm perform transactions that involve any of these triggering activities on behalf of a client (on a compensated or non-compensated basis)? a. receiving, paying funds or virtual currency b. purchasing or selling real property, or immovable or business assets, or entities c. transferring funds, virtual currency or securities by any means d. giving instructions in connection with any of the above (a, b, or c)	Yes	Performing any triggering activity, for any fees or no fees, gives rise to obligations defined in the AML/ATF legislation, unless exceptions apply. Receiving client fees does not itself constitute a triggering activity. Proceed to question 4.
	No	If the firm performs no triggering activity, no obligations arise from the AML/ATF legislation by virtue of being an accounting firm. 
4. Are all triggering activities performed in connection with assurance engagements or as part of receiver/trustee/monitor in bankruptcy appointments?	Yes	If all triggering activities are performed in connection with assurance engagements or as part of receiver/trustee/monitor in bankruptcy appointments, obligations defined by the AML/ATF legislation are not applicable. 
	No	If any one triggering activity is conducted that is not performed in connection with assurance engagements or as part of trustee in bankruptcy appointments, obligations defined by the AML/ATF legislation are applicable. <div style="background-color: black; color: white; padding: 2px; text-align: center; font-weight: bold;">LEGISLATION APPLICABLE</div>

3.4 Determination of triggering activities

Once it is determined that you are an accountant or an accounting firm, there is an ongoing risk that you or your firm conducts a triggering activity (even if it is determined at a point in time that no triggering activity has occurred in the past or is not expected in the future). The engagement in one single triggering activity gives rise (with some exceptions) to the full scope of obligations under the AML/ATF legislation applicable to accountants and accounting firms.

Once an accountant or accounting firm ceases to be involved in triggering activities, even after only engaging in a sole triggering activity, there also remains an obligation to keep records for five years depending on the type of record. The AML/ATF legislation is clear⁴⁰ about the obligation to maintain records once you are engaged in a triggering activity.⁴¹

Given the extent of effort required to maintain a compliance program, and the significant consequences for non-compliance, accounting firms should be vigilant in advance of performing any triggering activities.

3.5 A few important definitions and acronyms

The definitions used in this guide are those derived from the AML/ATF legislation, FINTRAC's glossary and other guidance.⁴² Below are several useful terms and acronyms that have been employed frequently throughout this guide.

3.5.1 Definitions

Affiliated entity – For purposes of the PCMLTFR, means an entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated.

Attempted transaction – Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a \$10,000 cash deposit. [Note: In the case of accountants or an accounting firm, since the term “deposits” does apply in the context of an accounting engagement, the example would refer to a receipt of \$10,000 or more in cash or virtual currency].

Authentic – In respect of verifying identity, means genuine and having the character of an original, credible and reliable document or record. [This means that accountants and accounting firms can rely on scanned and photocopied documents].⁴³

Beneficial owners – Are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25 per cent or more of i) the shares of a corporation or ii) an entity

40 PCMLTFR sections 144 to 149

41 For more information record-keeping obligations and retention periods, refer to Section 4.3.

42 FINTRAC, *Guidance Glossary*, May 4, 2021

43 The prohibition on the use of scanned/photocopied documents has been repealed and the requirement for an original document was amended on June 25, 2019 to require instead an “authentic, valid and current” document.

other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who own(s) or control(s) the entity.

Business relationship⁴⁴ – Occurs the second time that accountants or accounting firms are required to verify the identity of the client under the AML/ATF legislation.

Cash – Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada.⁴⁵

Client – A person or entity that engages in a financial transaction with another person or entity.⁴⁶

Close associate (of a politically exposed domestic person, a politically exposed foreign person or a head of an international organization is not defined in the AML/ATF legislation. FINTRAC provides in its guidance⁴⁷ some examples that are useful in making such a determination.) – A close associate can be a person who is connected to a PEP or HIO for personal or business reasons. Examples of relationships that could indicate that someone is a close associate (personal or business) could include, but are not limited to, persons who: are the business partners of, or who beneficially own or control a business with, a PEP or HIO; are in a romantic relationship with a PEP or HIO; are involved in financial transactions with a PEP or a HIO; serve as prominent members of the same political party or union as a PEP or HIO; serve as a member of the same board as a PEP or HIO; carry out charitable works closely with a PEP or HIO; or are listed as joint on a policy where one of the holders may be a PEP or HIO.

Once you determine that a person is the close associate of a PEP or HIO, they remain a close associate until they lose that connection.

Compliance officer – The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program.

44 PCMLTFR paragraph 4.1(b)

45 PCMLTFR subsection 1(2)

46 PCMLTFA section 2(1)

47 FINTRAC, *Politically exposed persons and heads of international organizations guidance*. May 4, 2021

Compliance policies and procedures – Written methodology outlining the obligations applicable to your business under the AML/ATF legislation and the corresponding processes and controls you put in place to address your obligations.

Currency conversion rate – See “Foreign currency or virtual currency.”

Current – In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified.

Distributed ledger – For purposes of section 151 of the PCMLTFR, it means a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities.

Entity – A body corporate, a trust, a partnership, a fund or an unincorporated association or organization.⁴⁸

Facts – Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client’s financial history.

Family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is (a) Their spouse or common-law partner; (b) their child; (c) their mother or father; (d) the mother or father of their spouse or common-law partner; or (e) a child of their mother or father.

Fiat currency – A currency that is issued by a country and is designated as legal tender in that country.⁴⁹

Financial entity – Defined as:

- a. an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act (e.g., banks savings and credit unions, caisses populaires, trust and loan companies)
- b. a financial services cooperative

48 PCMLTFA subsection 2(1)

49 PCMLTFR subsection 1(2)

- c. a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:
 - i. loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy, and the loan is secured by the value of an insurance policy
 - ii. loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy
 - iii. advance payments to which the policy holder is entitled that are made to them by the insurer
- d. a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central
- e. a department, or an entity that is an agent of Her Majesty in right of Canada or an agent or mandatary of Her Majesty in right of a province when it carries out an activity referred to in section 76 of the PCMLTFR

The exact list of entities are described in the PCMLTFA.⁵⁰

Foreign currency or virtual currency⁵¹ – If a transaction is conducted in a foreign currency or virtual currency, the amount of the transaction must be converted into Canadian dollars using: (a) the exchange rate that is published by the Bank of Canada for that foreign currency or virtual currency and that is in effect at the time of the transaction; or (b) if no exchange rate is published by the Bank of Canada for that foreign currency or virtual currency, the exchange rate that the person or entity would use in the ordinary course of business at the time of the transaction.

Funds – (a) Cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash. For greater certainty, it does not include virtual currency.⁵²

50 PCMLTFA subsections 5(a), (b) and (d) to (f)

51 PCMLTFR section 125

52 PCMLTFR subsection 1(2)

Head of an international organization⁵³ – A person who, at a given time, holds – or has held within five years before that time⁵⁴ – the office or position of head of an international organization that is established by the governments of states or the head of an institution of any such organization or an international sports organization.

Listed person – Anyone on a list published in the Schedule⁵⁵ of the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* issued under the *United Nations Act*. A listed person includes an individual, a corporation, a trust, a partnership or fund or an unincorporated association or organization that is believed to: have carried out, attempted to carry out, participated in or facilitated a terrorist activity; or be controlled directly or indirectly by, be acting on behalf of, at the direction of, or in association with any individual or entity conducting any of the above activities.

Mandatory – A person who acts, under a mandate or agreement, for another person or entity.

Ongoing monitoring – When you enter into a business relationship with a client, you must periodically conduct ongoing monitoring of that business relationship:⁵⁶

- based on a risk assessment established as part of your compliance program that was undertaken by assessing and documenting the risk, and taking into consideration the risk related to:
 - your clients and business relationships
 - your products, services and delivery channels
 - the geographic location of your activities
 - any other relevant factor

for the purpose of:

- detecting, when there are reasonable grounds to suspect, any transactions related to the commission or the attempted commission of a money laundering offence or to the commission or the attempted commission of a terrorist activity financing offence⁵⁷

53 PCMLTFA subsection 9.3(3)

54 PCMLTFR subsection 2(2)

55 *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360*, September 16, 2021.

56 FINTRAC *Ongoing monitoring requirements*, February 17, 2021

57 PCMLTFA section 7

- keeping client identification information, beneficial ownership⁵⁸ and business relationship⁵⁹ up to date⁶⁰
- reassessing the level of risk associated with your client's transactions and activities
- determining whether transactions or activities are consistent with the information obtained about your client, including the risk assessment of your client.

Politically exposed domestic person⁶¹ – A person who, at a given time, holds – or has held within five years within that time⁶² – one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k) in a municipal government:

- Governor General, lieutenant governor or head of government
- member of the Senate or House of Commons or member of a legislature of a province
- deputy minister or equivalent rank
- ambassador, or attaché or counsellor of an ambassador
- military officer with a rank of general or above
- president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province
- head of a government agency
- judge of an appellate court in a province, the Federal Court of Appeal, or the Supreme Court of Canada
- leader or president of a political party represented in a legislature
- holder of any prescribed office or position, or
- mayor

Politically exposed foreign person⁶³ – A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

- head of state or head of government
- member of the executive council of government or member of a legislature
- deputy minister or equivalent rank
- ambassador, or attaché or counsellor of an ambassador
- military officer with a rank of general or above

58 PCMLTFR section 138

59 PCMLTFR section 145

60 PCMLTFR section 123.1 (b)

61 PCMLTFA subsection 9.3(3)

62 PCMLTFR subsection 2(2)

63 PCMLTFA subsection 9.3(3)

- f. president of a state-owned company or a state-owned bank
- g. head of a government agency
- h. judge of a supreme court, constitutional court or other court of last resort
- i. leader or president of a political party represented in a legislature, or
- j. holder of any prescribed office or position

Public body – Refers to:

- a. a department or an agent of Her Majesty in right of Canada or an agent or mandatary of Her Majesty in right of a province
- b. an incorporated city, town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body or an agent of any of them
- c. an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or any agent of such an organization

Reasonable measures – The requirement to take steps to collect certain information, even if taking those steps did not result in the desired information being obtained. For example, according to FINTRAC guidance⁶⁴ this can include doing one or more of the following: asking the client, conducting open-source searches, or consulting commercially available information.

Risk assessment – The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact.

Senior officer in respect of an entity – If applicable, refers to (a) a director of the entity who is one of its full-time employees; (b) the entity’s chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or (c) any other officer who reports directly to the entity’s board of directors, chief executive officer or chief operating officer.⁶⁵

Source of funds or of virtual currency (VC) – The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may

64 FINTRAC, *Guidance Glossary*, May 4, 2021

65 PCMLTFR subsection 1(2)

have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc.⁶⁶

Source of wealth – The origin of a person’s total assets that can be reasonably explained, rather than what might be expected. For example, a person’s wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc.⁶⁷

Third-party – Any individual or entity that instructs someone to act on their behalf for a financial activity or transaction.⁶⁸

Training program – A written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the PCMLTFA and its associated regulations.

Transactions that are deemed to be single⁶⁹ – If an accountant or accounting firm that reports a LCTR, LVCTR or keeps a large cash or a large virtual currency transaction record, receives amounts in cash or virtual currency that total \$10,000 or more in two or more transactions that are made within 24 consecutive hours, those transactions are deemed to be a single transaction of \$10,000 or more if that accountant or accounting firm knows that

- a. the transactions are conducted by the same person or entity
- b. the transactions are conducted on behalf of the same person or entity, or
- c. the amounts are for the same beneficiary

In the case of the Large Virtual Currency Transaction Report (LVCTR) or the large virtual currency transaction record, paragraph (c) does not apply if the beneficiary is a public body; a corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated

66 FINTRAC, *Guidance Glossary*, May 4, 2021

67 Ibid

68 Ibid

69 PCMLTFR section 126 and subsections 129(1) and (2)

under subsection 262(1) of the *Income Tax Act* and that operates in a country that is a member of the FATF; or an administrator of a pension fund that is regulated under federal or provincial legislation.

Valid – In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes.⁷⁰

Very large corporation or trust – A corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the *Income Tax Act* and that operates in a country that is a member of the FATF.⁷¹

Virtual currency –

- a. a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
- b. a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).⁷²

3.5.2 Acronyms

Here is a list of commonly used acronyms in the Canadian AML/ATF community of practitioners.

AML/ATF – Anti-money laundering and anti-terrorist financing. This acronym is most often used in Canada by the Department of Finance Canada.⁷³ In international contexts, such as the FATF, this term is equivalent to the acronym AML/CFT, meaning anti-money laundering and combatting the financing of terrorism.⁷⁴

CSIS – Canadian Security Intelligence Service

70 FINTRAC, *Guidance Glossary*, May 4, 2021

71 FINTRAC, *Guidance Glossary*, May 4, 2021, and PCMLTFR paragraph 154(2)(n).

72 PCMLTFR subsection 1(2)

73 Department of Finance Canada, *Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, February 7, 2018

74 FATF, *Anti-money laundering and counter-terrorist financing measures*, September 15, 2016

FATF – Financial Action Task Force

FINTRAC – Financial Transactions and Reports Analysis Centre of Canada

HIO – Head of an International Organization

LCTR – Large cash transaction report, although the PCMLTFR refers to this report in its Schedule 1 as “Report with Respect to Receipt of Cash.”

LVCTR – Large Virtual Currency Transaction Report although the PCMLTFR refers to this report in its Schedule 4 as “Report with Respect to Receipt of Virtual Currency.”

PCMLTFA – *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

PCMLTFAMPR – Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations

PCMLTFR – Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations

PCMLTFSTRR – Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transactions Reporting Regulations

PEDP – Politically Exposed Domestic Person

PEFP – Politically Exposed Foreign Person

PEP – Politically Exposed Person. It is meant to designate both domestic and foreign politically exposed persons.

RBA – Risk-based approach

RGS – Reasonable grounds to suspect

STR – suspicious transaction report, although the PCMLTFSTRR refers to this report in its Schedule 1 as “Suspicious Transaction or Attempted Transaction Report.”

TPR – Terrorist Property Report, although PCMLTFSTRR refers to this report in its Schedule 2 as “Terrorist Group or Listed Person Property Report.”

RCMP – Royal Canadian Mounted Police

CHAPTER 4

Engaged in triggering activities, now what?

Accountants and accounting firms that engage in triggering activities are subject to the obligations of the AML/ATF legislation.⁷⁵ There are five broad AML/ATF legislation obligations to meet:

1. implement and maintain a compliance program
2. know your client
3. keep records
4. file reports
5. follow Ministerial directives and transaction restrictions/prohibitions

FINTRAC may contact you to ensure compliance with these AML/ATF obligations. To assess compliance, FINTRAC has the authority to examine your records and inquire into your business affairs. To carry out its compliance activities, FINTRAC conducts on-site or desk-based examinations.

4.1. Implement and maintain a compliance program

The first obligation, implementing and maintaining a compliance program,⁷⁶ is a preventive measure that aims to reduce the risk that the accountant or accounting firm will inadvertently be used for ML/TF purposes. It is intended to ensure your compliance under the AML/ATF legislation. A compliance program forms the basis for meeting all of your reporting, record keeping, client identification and other know-your-client requirements under the AML/ATF legislation. It is the immediate initiative you should address if you are planning to be engaged in a triggering activity. As soon as you have

⁷⁵ FINTRAC, *Accountants*, July 12, 2021

⁷⁶ See Chapter 6.

determined that you are an accountant or an accounting firm engaged in a triggering activity, you must have a compliance program in place. The implementation and maintenance of a compliance program includes six obligatory requirements, which are detailed in Chapter 6.⁷⁷

FINTRAC examination of the compliance program⁷⁸

As part of a FINTRAC examination, your compliance program will likely be reviewed. A detailed description of the implementation of a compliance program is provided in Chapter 6 including a summary of the areas that FINTRAC may focus upon during a compliance examination.⁷⁹

4.2 Know your client

The objective of “knowing your client” obligations is to ensure that you know who you are dealing with as a client and that you can take appropriate AML/ATF risk reduction measures if needed. It is done by identifying and verifying your client’s identity, assessing risk and monitoring your client on an ongoing basis. It is fundamental to meeting the AML/ATF legislation by preventing and detecting potential ML/TF and reduces legal, financial, reputational, professional and personal risks for accountants and accounting firms.

“Knowing your client” also means monitoring your client’s transactions and any changes in the nature and type of business conducted with you. The key obligations in “knowing your client” are:

1. verifying the identity of a person and the existence of an entity
2. determining business relationships and ongoing monitoring
3. meeting beneficial ownership requirements
4. determining if a third-party is giving instructions
5. determining politically exposed persons and heads of international organizations requirements

⁷⁷ PCMLTFR subsection 156(1)

⁷⁸ Throughout this guide there are areas highlighted in blue with the title **FINTRAC Examination**. The information provided in these highlighted areas is sourced from FINTRAC’s assessment manual. They represent the topics and issues FINTRAC may examine and focus upon when FINTRAC officers conduct either a desk review or an on-site examination.

⁷⁹ FINTRAC, *Assessment manual*, March 21, 2022

4.2.1 Verify the identity of a person and verify the identity of an entity

Verifying the identity of a person or entity means using the methods described in FINTRAC's guidance.⁸⁰ The purpose of client identification in the AML/ATF legislation is to verify the identity of the **person** (e.g., name, address, date of birth, nature of principal business or occupation) with whom you are dealing, or in the case of an entity, a client **other than a person**, to verify its existence (a corporation, or other than a corporation) or verify the identity of the individual who is dealing on behalf of the entity (with reference to corporate/other entity documentation).

The meaning of **person**⁸¹ in the AML/ATF legislation is that of an individual (natural person) whereas the meaning of an **entity**⁸² is a body corporate, a trust, a partnership, a fund or an unincorporated association or organization.

Verification of the client's identity must occur **at the time the transaction takes place** when the client is a **person**.⁸³ When, the client is an **entity**, verification of the client's identity should take place **within 30 days after the day on which the transaction is conducted**.⁸⁴

In instances where funds are received unexpectedly and without the client present, the accountant or accounting firm should verify the client's identity prior to processing or returning the funds (both to meet regulatory obligations and to establish ownership over the property).

The determination and verification of the identity of a client (person or entity) is triggered when there is a requirement to keep records (and report).⁸⁵

The identity must be determined and verified in the following circumstances:⁸⁶

- Receipt of funds record.⁸⁷ A receipt of funds record **must be completed when you receive \$3,000 or more in funds. Exception:** You do not have to verify the identity of a person or entity for the receipt of \$3,000 or more in funds, if the funds are from a client that is a financial entity or a public body, or from a person acting on behalf of a client that is a financial entity, a public body, a very large corporation or a subsidiary

80 FINTRAC, *Methods to verify the identity of persons and entities*, September 27, 2021

81 PCMLTFA subsection 2(1)

82 Ibid

83 PCMLTFR paragraph 105(7)(a)

84 PCMLTFR paragraph 109(4)(i)

85 FINTRAC, *Record keeping requirements for accountants*, August 4, 2021

86 FINTRAC, *When to verify the identity of persons and entities – Accountants*, August 4, 2021

87 PCMLTFR paragraphs 52(a) and (b)

of those types of entities, if the financial statements of the subsidiary are consolidated with those of the public body, very large corporation or trust.⁸⁸

- Large cash transactions. A large cash transaction record⁸⁹ must be completed **at the time of the transaction**⁹⁰ when there is a receipt of \$10,000 or more in cash in a single transaction (large cash transaction record⁹¹ and large cash transaction report⁹²). The large cash transaction record is subject to the 24-hour rule.⁹³

Exception: You do not have to verify the identity of a person or entity that conducts a large cash transaction if you receive the cash from a client that is a financial entity or a public body, or from a person who is acting on behalf of a client that is a financial entity or public body.⁹⁴

- Large virtual currency transactions. A large virtual currency record must be completed **at the time of the transaction for the large virtual currency transaction record**.⁹⁵ When there is a receipt of \$10,000 or more in virtual currency in a single transaction (Large virtual currency record⁹⁶ and large virtual currency transaction report).⁹⁷ The large virtual currency transaction record is subject to the 24-hour rule.⁹⁸

Exceptions: You do not have to verify the identity of a person or entity that conducts a large virtual currency transaction if you receive the virtual currency from a client that is a financial entity or a public body, or from a person who is acting on behalf of a client that is a financial entity or public body.⁹⁹ Also, when you receive virtual currency as compensation for the validation of a transaction that is recorded in a distributed ledger or you receive a nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information – you do not need to keep a large virtual currency transaction record and do not need to verify identity.¹⁰⁰

88 PCMLTFR paragraphs 154(2)(m), (n), and (o)

89 PCMLTFR paragraph 84(a)

90 PCMLTFR paragraph 109(4)(a)

91 Ibid

92 PCMLTFR subsections 152(1) (2) and (3) The requirement to report information on an item in a LCTR not marked with an asterisk * (mandatory items are marked with an asterisk) does not apply if after taking reasonable measures, you were unable to obtain the information.

93 FINTRAC [Transaction reporting guidance: the 24-hour rule](#), May 4, 2021

94 PCMLTFR section 50

95 PCMLTFR paragraph 109(4)(a)

96 PCMLTFR paragraph 84(b)

97 PCMLTFR subsections 152(1) (2) and (3) The requirement to report information on an item in a LVCTR not marked with an asterisk * (mandatory items are marked with an asterisk) does not apply if after taking reasonable measures, you were unable to obtain the information.

98 FINTRAC [Transaction reporting guidance: the 24-hour rule](#), May 4, 2021

99 PCMLTFR section 51

100 FINTRAC, [When to verify the identity of persons and entities – Accountants](#), September 27, 2021

- Suspicious transaction report. The identity must be verified **before the transaction or attempted transaction is reported to FINTRAC** under section 7 of the PCMLTFA¹⁰¹ and taking reasonable measures without tipping off the individual).¹⁰² You also do not have to take reasonable measures to verify the identity of the person if you have already verified the identity of the person or entity as required and have no doubts about the identification information.¹⁰³
- Terrorist, terrorist group or listed person report (reasonable measures).¹⁰⁴
- Determining if a third-party is giving instructions (reasonable measures for a large cash or large virtual currency transaction).¹⁰⁵

4.2.1.1 **FINTRAC examination**

FINTRAC has indicated that during an examination that it may assess the implementation of your client identification requirements.¹⁰⁶

FINTRAC examination of client identification requirements

FINTRAC may:

- review your policies and procedures to confirm that they give enough guidance to your employees or agents to verify the identity of your clients
- review client records and records of transactions to confirm that you apply these policies and procedures
- confirm, through a review of client records and records of transactions, that you verify the identity of persons and confirm the existence of entities in all situations where you are required to do so. These situations include, but are not limited to, when you:
 - open an account for a client, if applicable

¹⁰¹ PCMLTFR paragraph 109(4)(b)

¹⁰² PCMLTFR subsection 85(1) and (2) and PCMLTFSTR Schedule 1, Part D item 8, and Part E item 8. The requirement to verify the identity of the client does not apply if after taking reasonable measures, the person or entity is unable to obtain the information, or it will tip off the client to the completion of a STR.

¹⁰³ PCMLTFR subsection 155(1)

¹⁰⁴ PCMLTFSTR subsections 11(1) to (5). Schedule 1 refers to the STR and Schedule 2 refers to the TPR. Items identified in the STR and the TPR with an asterisk (*) are mandatory. The requirement to report information set out in in the STR and TPR does not apply in respect of information set out in an item of the STR and the TPR that is not marked with an asterisk if, after taking reasonable measures to do so, you are unable to obtain the information. The requirement to report information set out in the STR and TPR does not apply if you believe that taking the reasonable measures to obtain the information would inform a person or entity that conducts or attempts or proposes to conduct a transaction with you that the transaction and related information will be reported under section 7 (STR) or 7.1 of the Act (TPR). For greater certainty, although items in Schedules 1 and 2 are described in the singular, you must report all known information that falls within an item. You are not required to report information set out in any item of Schedule 1 or 2 that is not applicable in the circumstances.

¹⁰⁵ PCMLTFR subsections 134(1) to (3)

¹⁰⁶ FINTRAC, *Assessment manual*, March 21, 2022

- receive cash or virtual currency in the amount of \$10,000 or more from, or on behalf of, the same person or entity, or for the same beneficiary within a 24-hour period
- must create a client record
- must submit a suspicious transaction report
- are unable to obtain or confirm beneficial ownership information and must therefore take reasonable measures to identify the most senior managing officer of the entity and take special measures referred to in section 157 of the PCMLTFR (see Section 6.3.6 of this guide for more details)
- verify that you use the methods prescribed by law to verify the identity of a person or confirm the existence of an entity; and that, for persons, you rely on valid and current information, or authentic, valid and current documents to do so
- confirm that you verify the identity of your clients within the prescribed timeframe
- interview your employees and agents to assess their knowledge of client identification requirements

If you use an agent, another reporting entity or a foreign affiliated entity to help you verify the identity of clients, FINTRAC may:

- verify that you have a written agreement with the agent, reporting entity or the foreign affiliate
- verify that you receive all the required information from the agent, reporting entity or the foreign affiliate as soon as feasible
- verify how you ensure that your agent, reporting entity or foreign affiliate is using the verification methods required by law

FINTRAC's focus will be on the steps you take to ensure that you verify the identity of a person or an entity.

4.2.2 Determining business relationships and ongoing monitoring

4.2.2.1 Business relationship

A business relationship¹⁰⁷ is a relationship established between an accountant or an accounting firm (or any reporting entity) and a client to conduct financial transactions or provide services related to financial transactions. A business relationship is established for an accountant or accounting firm the **second time within a five-year period** that the accountant or accounting firm is required to verify the identity of the client when engaged in triggering activities. A business relationship ends when a period of at least five years has passed since the day of the last transaction that required you to verify the identity of the client.

You should determine that you have entered into a business relationship **as soon as possible** after verifying your client's identity for the second transaction or activity where you had the obligation to do so. As a best practice, you should make a business relationship determination within 30 calendar days of a second transaction or activity.

You do not enter into a business relationship that would otherwise have been formed if you are not required to verify the identity of a client due to an exception under the PCMLTFR. For example, if your requirement to verify identity does not apply because your client is a public body, a very large corporation, or a subsidiary of either of those, whose financial statements are consolidated, then a business relationship would not be formed.

However, a business relationship is formed in instances where you have the obligation to verify identity, even if the PCMLTFR allows you to not verify for a particular reason. This is because the underlying obligation to verify a client's identity still exists. This could occur as the result of a suspicious transaction or attempted transaction, or as the result of not having to re-verify the identity of a client

- **Suspicious transaction reporting (STR):**

When you are required to submit an STR to FINTRAC, you are required to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct the transaction. Despite whether your reasonable measures are unsuccessful, or if you believe taking reasonable measures would inform the person or entity that you are

107 PCMLTFR section 4.1 and FINTRAC, *Business relationship requirements*, August 4, 2021

filing an STR, this transaction must factor into your business relationship requirements, as either the first or second time you are required to verify the identity of a client.

- **Re-verifying identity:**
Your business relationship requirements must still factor in a transaction or activity for which you have the requirement to verify identity but choose not to because the PCMLTFR allow it. The PCMLTFR allow you to choose not to re-verify the identity of a client if:
 - you previously did so using the methods specified in the Regulations in place at the time
 - you have kept the associated records
 - you have no doubts about the information used

If you submitted a suspicious transaction report or a Terrorist Property Report to FINTRAC on two occasions for this client (including those below the \$3,000 threshold)¹⁰⁸ you will have had the obligation to verify the identity of the client twice, hence a business relationship would have been created. The establishment of a business relationship gives rise to the immediate obligation to keep a business relationship record (see Chapter 26 that sets out the “purpose and intended nature of the business relationship”).¹⁰⁹ FINTRAC provides in its guidance the following as examples of what could be used to describe the purpose and intended nature of the business relationship: “Transferring funds or securities,” or “Paying or receiving funds on behalf of client,” or “Purchasing or selling entities or business assets.”

As a best practice, to help you meet your “know your client” requirements and conduct ongoing monitoring of your business relationships, this record should also:

- describe your business dealings with the client
- include information that would help you anticipate the types of transactions and activities that the client may conduct. You could then use this information to identify unusual or suspicious transactions while conducting your ongoing monitoring.¹¹⁰

Establishing a business relationship also triggers the ongoing obligations¹¹¹ to periodically monitor the business relationship and keep an ongoing business relationship record (see Chapter 26)¹¹² recording the measures taken when

108 See Section 7.2 for additional information on business relationships

109 PCMLTFR section 145

110 FINTRAC, *Business relationship requirements*, September 27, 2021

111 PCMLTFR section 123.1

112 PCMLTFR subsection 146(1)

you conduct ongoing monitoring of the business relationship with that person or entity and of the information obtained from that ongoing monitoring on a risk-sensitive basis.

All of the measures and the definition of purpose and intended nature of the business relationship are with reference only to triggering activities. Non-triggering activities (such as the performance of an audit engagement) are to be excluded from the analysis. As a best practice, to help you meet your “know your client” requirements and conduct ongoing monitoring of your business relationships, this record should also describe your business dealings with the client; and include information that would help you anticipate the types of transactions and activities that the client may conduct. You could then use this information to identify unusual or suspicious transactions while conducting your ongoing monitoring.

4.2.2.2 Ongoing monitoring

Ongoing monitoring is a process that you must develop and use to review all the information you have obtained about the clients with whom you have a business relationship.¹¹³ As noted above the purpose of ongoing monitoring is to:

- detect any suspicious transactions that you are required to report to FINTRAC
- keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date
- reassess the level of risk associated with your client’s transactions and activities
- determine whether transactions or activities are consistent with the client information you obtained and your risk assessment of the client

Your process for conducting ongoing monitoring could include the monitoring of an individual client or of groups of clients. When you enter into a business relationship with a client (individual or groups of clients) you must periodically conduct ongoing monitoring of that business relationship, based on your risk assessment.

113 FINTRAC, *Ongoing monitoring requirements*, September 27, 2021

The frequency at which you conduct ongoing monitoring will depend on the risk level assigned to clients in your risk assessment. For example, clients identified as posing a low risk may require less frequent ongoing monitoring whereas those in your high-risk category will require that you take enhanced measures.

You must take enhanced measures and conduct enhanced ongoing monitoring of a client that you have identified as posing a high risk in your risk assessment. This means that you must take extra measures in addition to what is required, as appropriate for the level of client risk (see Section 4.2.2.6 of this guide). This includes taking additional measures for client identification, conducting enhanced ongoing monitoring (e.g., more frequent monitoring), and taking any other enhanced measure you identify as appropriate.

You could consider the following methods to conduct enhanced ongoing monitoring of your high-risk clients:

- reviewing transactions based on an approved schedule that involves management sign-off
- developing reports and reviewing these reports of high-risk transactions more frequently
- flagging certain activities or those that deviate from your expectations and raise concerns, as necessary
- setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review, or
- reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships

Measures undertaken to conduct ongoing monitoring, as well as findings and outcomes, must be documented. Ideally, all ongoing monitoring for any given client is conducted on the same cycle to achieve efficiencies. You may consider using the sample form described in Section 26.1.2 “Sample – Record of Business Relationship Information” as a record. You must keep a record of the ongoing monitoring measures taken and the information obtained from that ongoing monitoring for at least five years from the date the record was created.

You are not required to conduct ongoing monitoring when your business relationship with a client ends. You are not required to conduct **enhanced** ongoing monitoring when your business relationship ends **or** when, based on your risk assessment, you no longer consider a client to pose a high risk.

When you no longer consider a client high-risk, you are still required to conduct ongoing monitoring of the client at the frequency determined by the client's new risk rating.

4.2.2.2.1 Ongoing monitoring records

You must keep records of the measures you take **and** of the information obtained from the ongoing monitoring of your clients with whom you have a business relationship. This includes:

- your processes in place to perform ongoing monitoring
- your processes in place to perform the enhanced ongoing monitoring of high-risk clients
- your processes for recording the information obtained as a result of your ongoing monitoring
- your processes for recording the information obtained as a result of your enhanced ongoing monitoring of high-risk clients
- the information obtained as a result of your ongoing monitoring and enhanced ongoing monitoring of high-risk clients

You must outline the measures you use to conduct the ongoing monitoring of your business relationships in your policies and procedures, which can form part of your ongoing monitoring records. However, the information you obtain as a result of your ongoing monitoring is likely to be specific to a particular business relationship and not captured in your policies and procedures, so it should be documented separately. You can document and update the information you obtain through your ongoing monitoring activities across several records. For example, updates to the client identification, beneficial ownership or business relationship information you have, could be recorded in any file you maintain on a client.¹¹⁴

4.2.2.2.2 FINTRAC examination

FINTRAC has indicated that during an examination, it may assess the implementation of your business relationship and ongoing monitoring requirements.¹¹⁵

¹¹⁴ FINTRAC, *Ongoing monitoring requirements*, September 27, 2021

¹¹⁵ FINTRAC, *Assessment manual*, March 21, 2022

FINTRAC examination of business relationship and ongoing monitoring requirements

FINTRAC may:

- verify that you used the results of your risk assessment to determine how often you monitor your clients, or which transactions you will monitor more often or more closely. FINTRAC focuses on situations where you may not be adequately monitoring a client or transactions that you consider pose a high risk or to be suspicious (see Section 4.2.6 of this guide for more information on what to do when you have identified high-risk clients).
- verify that you monitor your high-risk business relationships more frequently to identify suspicious transactions and apply special measures to mitigate risks
- review business relationships that you have ranked as posing a low or medium risk to determine whether this ranking is appropriate. FINTRAC will compare your low-risk and medium-risk clients to your high-risk clients in light of the criteria you have established to identify high-risk situations.
- review your ongoing monitoring of low- and medium-risk business relationships to ensure they are adequately monitored.
- verify that you identify and address inconsistencies between a client's actual and expected transactional activity. Transactional activity inconsistency is a common indicator of money laundering and terrorist activity financing.

FINTRAC will focus on ensuring you have an adequate ongoing monitoring process in place.

As a best practice, your policies and procedures should include the frequency at which you will conduct ongoing monitoring of your clients, based on your risk assessment for a client or group of clients.

4.2.3 Beneficial ownership requirements

Concealment of beneficial ownership information is a technique used in money laundering and terrorist financing. Identifying the ultimate beneficial owners of an entity removes the anonymity of individuals behind transactions and account activity. There is a global movement to collect beneficial ownership in company records. Some countries make select beneficial ownership information accessible in a public register.

In June 2019, federally incorporated companies (privately held corporations) were required under the *Canada Business Corporations Act* (CBCA) to collect and maintain beneficial ownership information¹¹⁶ in their own records. Several provinces and territories have agreed to follow suit through corporations legislation.

CPA Canada has supported efforts to make beneficial ownership accessible to accountants and accounting firms by way of a publicly accessible register while balancing the privacy rights of Canadians.¹¹⁷ In the federal Budget 2021,¹¹⁸ the government proposed to provide \$2.1 million over two years to Innovation, Science and Economic Development Canada to support the implementation of a publicly accessible corporate beneficial ownership registry by 2025.

What are beneficial owners? Beneficial owners are the individuals who directly or indirectly own or control 25 per cent or more of a corporation or an entity other than a corporation. In the case of a trust, they are the trustees, the known beneficiaries and the settlors of the trust. If the trust is a widely held trust or a publicly traded trust, they are the trustees and all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust.¹¹⁹

Beneficial owners cannot be other corporations, trusts or other entities. They must be the individuals who are the owners or controllers of the entity. It is important to consider and review the names found on official documentation in order to confirm the accuracy of the beneficial ownership

116 In the Canada Business Corporations Act the expression “Individuals with Significant Control” is used to mean a beneficial owner.

117 CPA Canada, *Accountants offer valuable views in beneficial ownership registry discussion with new international report*, May 28, 2020

118 Government of Canada, *Budget 2021*, p. 309, April 19, 2021

119 PCMLTFR subsection 138(1)

information. It may be necessary to search through many layers of information in order to confirm who are the beneficial owners, as the names found on official documentation may not always reflect the actual beneficial owners.¹²⁰

At the time you verify the identity of an entity, you must also obtain information about its beneficial ownership.¹²¹ In all cases (except for not-for-profit organizations), you must collect information establishing the ownership, control and structure of the entity.¹²² If you established a business relationship with that client, you must also confirm the accuracy of the beneficial ownership information in the course of ongoing monitoring. You must keep a record of the beneficial ownership information you obtain and of the measures you take to confirm the accuracy of the information for at least five years from the day the last business transaction is conducted¹²³ as follows:

Table 3

Entity Type	Information to Collect	
Corporation ¹²⁴	Names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation	In all cases, you must obtain information establishing the ownership, control and structure of the entity
Widely held or publicly traded trust ¹²⁵	Names of all trustees of the trust and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust	In all cases, you must obtain information establishing the ownership, control and structure of the entity
Trust ¹²⁶	Names and addresses of all trustees and all known beneficiaries and settlors of the trust	In all cases, you must obtain information establishing the ownership, control and structure of the entity

120 FINTRAC, *Beneficial ownership requirements*, September 27, 2021

121 Ibid.

122 PCMLTFR paragraph 138(1)(d)

123 PCMLTFR paragraph 148(1)(b)

124 PCMLTFR paragraph 138(1)(a)

125 PCMLTFR paragraph 138(1)(a.1)

126 PCMLTFR paragraph 138(1)(b)

Entity Type	Information to Collect	
Entity other than a corporation or trust ¹²⁷	The names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity	In all cases, you must obtain information establishing the ownership, control and structure of the entity
Not-for-profit organization ¹²⁸	<p>Determine if it is a charity registered with the CRA under the <i>Income Tax Act</i>, or</p> <p>An organization, other than a charity registered with the CRA under the <i>Income Tax Act</i>, that solicits charitable donations from the public.</p>	

In situations where no individual directly or indirectly owns or controls 25 per cent or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust, you must keep a record of the measures you took to confirm the accuracy of the information, as well as the information you obtained in order to reach that conclusion. The date you took the measures should also be included as a best practice.

FINTRAC’s guidance on beneficial ownership requirements provides examples of records to be kept for several of the situations described in Table 3 above. You may also use the form provided in Section 25.7 “Sample Record of Beneficial Ownership” as an example.

4.2.3.1 Reasonable measures to obtain beneficial ownership information and confirm its accuracy

You must take reasonable measures¹²⁹ to confirm the accuracy of the beneficial ownership information when it is first obtained and in the course of ongoing monitoring of business relationships. You must keep a record that sets out the information and the measures taken to confirm the accuracy of the information.

¹²⁷ PCMLTFR paragraph 138(1)(c)

¹²⁸ PCMLTFR subsection 138(5)

¹²⁹ FINTRAC *Guidance Glossary* – Reasonable measures means steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following: asking the client, conducting open-source searches, retrieving information already available, including information held in non-digital formats, or consulting commercially available information.

Obtaining beneficial ownership information

To obtain beneficial ownership information, which includes information on the ownership, control and structure, you could have the entity provide it, either verbally or in writing, or you could search for publicly available information.

For example:

- the entity can provide you with official documentation
- the entity can tell you the beneficial ownership information and you can write it down for record keeping purposes, or
- the entity can fill out a document to provide you with the information¹³⁰

If you are unable to obtain the beneficial ownership information, to keep it up to date in the course of ongoing monitoring of business relationships or to confirm its accuracy, you must:

- take reasonable measures to verify the identity of the entity's chief executive officer or the person who performs that function
- apply special measures (enhanced measures) for high-risk clients. These measures are referred to in section 157 of the PCMLTFR which are:
 - a. taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity
 - b. taking any other enhanced measure to mitigate the risks, including
 - i. ensuring, at a frequency appropriate to the level of risk, that client identification information and beneficial information is up to date
 - ii. conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships to:
 - a. detect suspicious transactions
 - b. keep client identification information, beneficial ownership and business relationship information up to date
 - c. reassess the level of risk associated with the client's transactions and activities
 - d. determine whether transactions or activities are consistent with the information obtained about their client, including the risk assessment of the client

¹³⁰ FINTRAC, *Beneficial ownership requirements*, August 4, 2021

The AML/ATF legislation does not require that you verify the identity of the chief executive officer or of the person who performs that function in accordance with the prescribed methods.¹³¹ However, you could use one of the methods outlined in FINTRAC’s guidance on “Methods to verify the identity of persons and entities”¹³² which are also described in Chapter 23 of this guide.

Additionally, there is no record keeping obligation if you have identified the chief executive officer or a person who performs that function using the prescribed methods to verify identity. However, during a FINTRAC examination, you could be asked to demonstrate the reasonable measures that you took to identify the chief executive officer or person who performs that function.

Confirming the accuracy of beneficial ownership information

You must take reasonable measures to confirm the accuracy of the beneficial ownership information that you obtain.¹³³ These reasonable measures cannot be the same as the measures you used to obtain the information. Your reasonable measures could include referring to official documentation or records. For example, for a corporation or other entity, you could refer to records such as, but not limited to, the: minute book, securities register, shareholders register, articles of incorporation, annual returns, certificate of corporate status, shareholder agreements, partnership agreements, or board of directors’ meeting records of decisions.

It is also acceptable to have a client sign a document to confirm the accuracy of the beneficial ownership information you obtained, which includes information on ownership, control and structure. In this case, it is possible for one document to be used to satisfy the two steps—namely to obtain the information and to confirm its accuracy by means of the signature.

In the case of a trust, you could confirm the accuracy of the information by reviewing the trust deed, which should provide you with the information needed. Other reasonable measures can include asking the client to provide supporting official documentation, conducting an open-source search, or consulting commercially available information.

¹³¹ FINTRAC, *Beneficial ownership requirements*, August 4, 2021

¹³² FINTRAC, *Methods to verify the identity of persons and entities*, November 19, 2021

¹³³ PCMLTFR subsection 138(2)

As a best practice, you should also confirm whether a not-for-profit organization is a charity registered with the CRA by consulting the charities listing on the CRA website.^{134 135}

The reasonable measures that you take to confirm the accuracy of beneficial ownership information, which includes ownership, control and structure information, must align with your risk assessment of the entity's risk for money laundering or terrorist activity financing offences. The reasonable measures you take with entities assessed to pose a high risk must go further to help you understand and confirm the beneficial ownership, as well as establish the overall ownership, control, and structure of that entity.

The reasonable measures that you take with entities that have complex business structures must go further to ensure that you are able to understand and confirm the accuracy of beneficial ownership, which includes establishing the ownership, control and structure of that entity. This does not mean, however, that you need to consider or treat a complex entity as posing a high risk. You need to choose reasonable measures that are appropriate to the situation.¹³⁶

What if there are no beneficial owners?¹³⁷

You may obtain information confirming that there is no individual who directly or indirectly owns or controls 25 per cent or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust. This is not the same thing as being unable to obtain the beneficial ownership information.

If you determine that there is no beneficial owner, you must keep a record of the measures you took and the information you obtained in order to reach that conclusion.¹³⁸ However, you are still required to obtain and take reasonable measures to confirm information about the ownership, control and structure of the entity.

4.2.3.2 Exceptions to beneficial ownership requirements

You do not have to obtain beneficial ownership information and take reasonable measures to confirm its accuracy for a group plan account held within a dividend or a distribution reinvestment plan. This includes plans

¹³⁴ FINTRAC, *Beneficial ownership requirements*, August 4, 2021

¹³⁵ Government of Canada, *List of Charities*, July 10, 2020

¹³⁶ FINTRAC, *Beneficial ownership requirements*, August 4, 2021

¹³⁷ Ibid

¹³⁸ PCMLTFR subsection 138(3)

that permit purchases of additional shares or units by the member with contributions other than the dividends or distributions paid by the plan sponsor, if the sponsor is an entity whose shares or units are traded on a Canadian stock exchange; and that operates in a country that is a member of the FATF.¹³⁹

The beneficial ownership requirements do not apply if you are not required to verify the identity of an entity under the PCMLTFR because of a related exception. This is because your obligation to verify identity for a particular transaction, activity or client does not apply in that circumstance.

4.2.3.3 FINTRAC examination

FINTRAC has indicated that during an examination, that it may assess the implementation of your beneficial ownership requirements.¹⁴⁰

FINTRAC examination of beneficial ownership requirements

FINTRAC may:

- verify that you have a process in place to obtain beneficial ownership information
- verify your records and the process you have in place to confirm the accuracy of the information obtained
- verify whether you take reasonable measures to identify the chief executive officer or the person who performs that function in the entity for which you are unable to obtain or confirm the beneficial ownership information, and treat the entity as posing a high risk and apply special measures referred to in section 157 of the PCMLTFR (also see Section 8.4 of this guide)
- verify whether you monitor the entities you consider to pose a high risk more frequently than other entities and apply special measures to mitigate the risks

FINTRAC will focus on ensuring that you are taking reasonable steps to confirm who the individuals are that own or control an entity.

¹³⁹ PCMLTFR subsection 138(6)

¹⁴⁰ FINTRAC, *Assessment manual*, March 21, 2022

4.2.4 Is a third-party giving instructions to your client?

The FATF, the Egmont Group organization (the international organization of financial intelligence units) and other anti-money laundering and anti-terrorist financing authoritative bodies have observed that third-parties have been used in several money laundering and terrorist financing cases.¹⁴¹ It is not uncommon for criminals to use third-parties as a method to evade detection by distancing themselves from the proceeds of crime.

A third-party is the person or entity that instructs another person or entity to conduct an activity or financial transaction on their behalf. As such, the third-party is the instructing party to the transaction or activity and is also understood to be the “on behalf of” party.

When you are determining whether a third-party is giving instructions, it is not about who owns or benefits from the money, or who is carrying out the transaction or activity, but rather about who gives the instructions to handle the money or conduct a transaction or particular activity. If you determine that the individual in front of you is acting on someone else’s instructions, that someone else is the third-party. For example, Jim is the third-party when he asks Alice to wire \$12,000 to a business account held by company ABC in country A.

When a person is acting on behalf of their employer, the employer is considered to be the third-party, unless the person is making a cash deposit to the employer’s business account.¹⁴²

When you receive an amount of \$10,000 or more in cash or in virtual currency¹⁴³ or keep a large cash transaction record or a large virtual currency transaction record you must take reasonable measures (Record of Reasonable Measures Taken to Determine a Third-party) to determine whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party.¹⁴⁴ Reasonable measures could include asking your client if they are acting at the instruction of another person or entity, or asking whether another person or entity will be instructing on the account. The steps you take to make a third-party determination must be documented in your compliance policies and procedures.

141 FINTRAC, *Third party determination requirements*, August 4, 2021

142 Ibid

143 The 24 hour-rule applies when recording and reporting a large cash transaction record and a large virtual currency transaction.

144 PCMLTFR subsection 134(1)

If you determine that the person from whom the cash or virtual currency is received is acting on behalf of a third-party, you must take reasonable measures to obtain the following information and keep a record of that information for at least five years following the date they were created:¹⁴⁵

- If the third-party is a **person** – their name, address, telephone number (not required if the third-party determination is made for a large cash transaction or large VC transaction), date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business.
- If the third-party is a **corporation or other entity** – its name, address, telephone number (not required if the third-party determination is made for a large cash transaction or large VC transaction), the nature of its principal business, its registration or incorporation number and the jurisdiction (province or state) and country of issue of that number.
- The **relationship** between the third-party and the following person or entity, as applicable:
 - the person who conducts the large cash transaction, or
 - the person who conducts the large VC transaction

The relationship between the person or entity and the third-party can be, for example, an accountant, broker, customer, employee, friend or relative. Making a third-party determination as required, will assist you in completing any report you submit to FINTRAC. Specifically, if you determine that a third-party is involved in any of the transactions or activities, then this information may help you in completing the ‘on behalf of’ section of any related report you send to FINTRAC.

If you are not able to determine whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party but there are reasonable grounds to suspect that they are, you must keep a record that:¹⁴⁶

- describes the reasonable grounds to suspect that they are acting on behalf of a third-party
- indicates:
 - when you receive cash or an amount of VC equivalent to \$10,000 or more and are required to submit an LCTR or LVCTR to FINTRAC or to keep a large cash or large virtual currency transaction record – **whether according to the person from whom the cash or VC is received, they are acting on their own behalf only**¹⁴⁷

145 PCMLTFR subsections 134(2), 135(2), 136(2), 137(2)

146 PCMLTFR subsection 134(3)

147 PCMLTFR subsection 134(3)(a)

Further explanations and a sample form (Third-party Determination Record When Receiving \$10,000 or More in Cash or Virtual Currency) is provided in this guide in Section 32.2 to capture the information required for the determination of a third-party, whether the measures were successful or not.

4.2.4.1 **FINTRAC examination**

FINTRAC has indicated that during an examination, it may assess the implementation of your third-party determination requirements.¹⁴⁸

FINTRAC examination of third-party determination requirements

FINTRAC may:

- Review your procedures, processes and controls for situations where you are not able to determine whether an account is to be used by, or on behalf of, a third-party when there are reasonable grounds to suspect that it would be.

FINTRAC will focus on ensuring that you are taking reasonable steps to determine whether there is a third-party to a transaction or giving instructions on an account.

4.2.5 **Business relationships with politically exposed persons (PEPs), their family members and close associates**

Note: References to PEPs include both foreign and domestic PEPs.

The AML/ATF legislation has identified specific requirements in dealing with a politically exposed foreign person (PEFP), a politically exposed domestic person (PEDP), a head of an international organization (HIO), their family members and their close associates¹⁴⁹ when you:

1. **Enter** into a business relationship (i.e., upon the second time you verify the identity of the person) with a PEFP, PEDP, HIO, a family member of one of those persons or a person who is closely associated one of these persons (see specific requirements in Section 15.2). In such a case you must take reasonable measures to determine whether a person with whom you enter into a business relationship is such a person.

¹⁴⁸ FINTRAC, *Assessment manual*, March 21, 2022

¹⁴⁹ Refer to the definitions of each of these terms in Section 3.5.1 in this guide. Also, Chapter 17 of this guide provides a link to FINTRAC's guidance on politically exposed persons, heads of international organizations, their family members and close associates.

2. **Have a business relationship and conduct periodic monitoring** of the business relationship you must take reasonable measures to determine whether the person with whom you have a business relationship is a PEFP, PEDP, HIO, a family member of one of those persons or a close associate (see specific requirements in Section 15.3).
3. **Detect a fact** that constitutes reasonable grounds to suspect **that a person with whom you have a business relationship** is a PEFP, PEDP or HIO, or a family member of, or a person who is closely associated with, one of those persons (see specific requirements in Section 15.4). In such a case you must take reasonable measures to determine whether they are such a person.

In all of these cases there are additional reasonable measures and/or special measures and record keeping requirements to be met. A table summarizing these requirements is provided in Chapter 15 - Appendix A: Summary table of requirements when dealing with a PEFP, PEDP, HIO, their family members or close associates.

4.2.5.1 **FINTRAC examination**

FINTRAC has indicated that during an examination, it may assess the implementation of the requirements related to business relationships with politically exposed persons, their family members and close associates.

FINTRAC examination of requirements related to business relationships with politically exposed persons, their family members and close associates

FINTRAC may:¹⁵⁰

- verify your records to confirm that you rate all your foreign politically exposed person clients as posing a high risk, as well as their family members and close associates
- review your records of PEDPs and HIOs, as well as those of their family members and close associates, to ensure that you have adequately assessed the level of risk posed by these clients. To do so, FINTRAC looks at a sample of these clients to see if they meet the criteria you have established to rate a client as posing a high risk
- verify whether you monitor your high-risk clients more frequently than your lower-risk clients and apply special measures

150 FINTRAC, *Assessment manual*, March 21, 2022

- review transaction records involving PEPs and HIOs, as well as their family members and close associates, to confirm that you are reporting suspicious transactions when required

FINTRAC will focus on ensuring that you are taking reasonable steps to find out if your clients are politically exposed persons or heads of international organizations (including family members and close associates), and for those who pose a high risk, FINTRAC will focus on the special measures you have in place.

4.2.6 Have you assessed your client as high risk?

When you established your compliance program, you conducted a risk assessment and documented the risk¹⁵¹ taking into consideration five important factors:

1. your clients and business relationships
2. your products, services, and delivery channels
3. the geographic location of your activities
4. any other relevant factor
5. If you intend on carrying out a new development or introduce a new technology that may have an impact on your clients, business relationships, products, services or delivery channels or the geographic location of your activities, you must assess and document the risk before doing so.¹⁵²

If you have assessed any of your clients as high risk, you must take special measures to mitigate the risk as prescribed in the AML/ATF legislation¹⁵³ and described as **enhanced measures** in FINTRAC's guidance.¹⁵⁴ As part of your compliance program these enhanced measures must be documented additional controls and processes that will be applied to high-risk clients, and must include taking:

- enhanced measures to verify the identity of persons and entities
- enhanced measures to keep client information up to date
- enhanced measures to keep beneficial ownership information up to date

151 PCMLTFR subsection 156(1)

152 PCMLTFR subsection 156(2)

153 PCMLTFR section 157

154 FINTRAC, *Compliance program requirements*, August 4, 2021

- enhanced measures to conduct ongoing monitoring of business relationships for the purposes of detecting and reporting suspicious transactions
- any other enhanced measures to mitigate the risks identified

Some examples of enhanced measures are outlined below:

- obtaining additional information on the client (e.g., occupation, volume of assets, information available through public databases, Internet, etc.)
- obtaining information on the source of funds or source of wealth of the client
- obtaining information on the reasons for intended or conducted transactions
- increased monitoring of transactions of higher-risk products, services, and channels
- gathering additional documents, data, or information; or taking additional steps to verify the documents obtained
- establishing transaction limits
- increasing internal controls of high-risk business relationships
- obtaining the approval of senior management at the transaction level for products and services that are new for that client

During a FINTRAC examination, you will need to demonstrate that you review your high-risk client information more frequently and keep all client information up to date. You must also be able to demonstrate the measures you have in place to mitigate risk where required. It is important to note that high-risk activities can occur outside of business relationships. As such, any client not in a business relationship that is assessed as posing a high risk of committing a money laundering or terrorist financing offence must also be subjected to enhanced measures.

You could consider the following methods to monitor high-risk situations:

- review transactions based on an approved schedule that involves management sign-off
- develop reports and perform more frequent reviews of reports that list high-risk transactions
- flag certain activities or activities that deviate from your expectations and elevate concerns as necessary
- set business limits or parameters regarding accounts or transactions that would trigger early warning signals and require a mandatory review
- review transactions more frequently against suspicious transaction indicators relevant to the business relationship

4.3 Keep records and copies of reports

As an accountant or accounting firm, you have record keeping obligations when you engage in triggering activities on behalf of any person or entity (other than your employer).

Notwithstanding a request from FINTRAC for compliance purposes, these records may also be requested through a judicial order by law enforcement to support an investigation of money laundering or terrorist activity financing. A record (or a copy) may be kept in a machine-readable or electronic form, so long as a paper copy can easily be produced.

Employees who keep records for you are not required to keep them after the end of their employment with you. The same is true for individuals in a contractual relationship with you, after the end of that contractual relationship. This means that you have to obtain and keep the records that were kept for you by any employee or contractor before the end of that individual's employment or contract with you.

There may be situations where you are required to keep records for purposes other than your requirements under the AML/ATF legislation. For example, a federal or provincial regulator for your sector may require you to keep records in addition to those described in this guidance. If this is the case, you must still meet the requirements described in this guidance. For example, the retention period for your records can be longer than what is described, but it cannot be shorter.

Accountants and accounting firms must keep the following records and copies of reports, subject to the exceptions in the AML/ATF legislation:

- receipt of funds record (refer to Chapters 8 and 22)¹⁵⁵
- record of verification of the identity of the client (for large cash transactions, large virtual currency transactions, suspicious transactions or attempted transactions and Terrorist Property Reports) (refer to Chapters 23 and 24)¹⁵⁶
- business relationship record (refer to Section 8.3 and to Chapter 26)¹⁵⁷
- ongoing business relationship record (refer to Section 8.3 and to Section 26.1.2)¹⁵⁸

155 PCMLTFR paragraphs 52(a) and (b)

156 PCMLTFR section 84, subsections 85 (1) and (2), and PCMLTFSTRR 12.1

157 PCMLTFR section 145

158 PCMLTFR subsection 146(1)

- record of reasonable measures to confirm the accuracy of beneficial ownership information (Refer to Section 8.3 and to Section 25.7)¹⁵⁹
- copy of large cash transaction report (Refer to Chapters 10 and 27)¹⁶⁰
- large cash transaction record (Refer to Section 10.8)¹⁶¹
- record of reasonable measures taken determining the third-party in a large cash or large virtual currency transaction (Refer to Section 32.2)¹⁶²
- record of grounds to suspect third-party involvement in a large cash/ large virtual currency transaction (Refer to Section 32.2)¹⁶³
- copy of Large Virtual Currency Transaction report (Refer to Chapter 28),¹⁶⁴
- large virtual currency transaction record (Refer to Section 10.7)¹⁶⁵
- copy of the suspicious transaction or attempted transaction report (Refer to Chapters 9 and 21)¹⁶⁶
- copy of the Terrorist Property Report (Refer to Chapters 11 and 29)¹⁶⁷ and
- record of PEP, HIO, Family and Close Associate When Receiving \$100,000 or More in Cash or Virtual Currency (Refer to Chapter 15 and Section 10.9.2)¹⁶⁸

The records above are listed in the table in Section 4.7 of this guide which summarizes when they are required in eight different scenarios/special events. Other records include the record of PEP, HIO, family and close associate when a business relationship is or may be involved (refer to Chapter 15 and Section 10.9.2).

4.3.1 Reasonable measures

The term “reasonable measures” refers to activities you are expected to undertake in order to meet certain obligations. The AML/ATF legislation explicitly states when you must take reasonable measures to meet an obligation. To further explain, reasonable measures means that you must take steps to collect certain information, even if taking those steps did not result in the desired information being obtained. For example, according to FINTRAC guidance¹⁶⁹ this can include doing one or more of the following:

- asking the client

159 PCMLTFR subsections 138(2) to (4)

160 PCMLTFR section 144

161 PCMLTFR section 50

162 PCMLTFR subsections 134(1) to (3)

163 PCMLTFR subsection 134(3)

164 PCMLTFR section 144

165 PCMLTFR section 51

166 PCMLTFR subsections 85 (1) and (2), and PCMLTFSTR subsection 12.1 and PCMLTFSTR Schedule 1, Part D item 8, and Part E item 8. The requirement to verify the identity of the client no longer applies if after taking reasonable measures, the person or entity is unable to obtain the information.

167 PCMLTFR section 144

168 PCMLTFR subsection 123(4)

169 FINTRAC, *Guidance Glossary*, May 5, 2021

- conducting open-source searches, or
- consulting commercially available information

These reasonable measures should be described in your compliance policies and procedures.

Retention: You must keep records of the reasonable measures taken for at least five years following the date they were created.

4.3.2 FINTRAC examination

FINTRAC has indicated that during an examination, it may assess the implementation of the record keeping requirements.¹⁷⁰

FINTRAC examination of record keeping requirements

FINTRAC may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the record keeping requirements.
- Review your client records and records of transactions to confirm that you put these policies and procedures into practice.
- Verify that you keep records as required by the AML/ATF legislation when reviewing your client records and records of transactions. Records may include the following, as applicable:
 - records of large cash transactions
 - records of large virtual currency transactions
 - records of suspicious transaction reports
 - reasonable measures records
 - records that you are required to keep under client identification and know your client requirements
- Verify that you keep the information that is required (for example, name, address, date of transaction, etc.) for each type of record. The information that you are required to keep is determined by the type of record that needs to be kept.
- Verify that your records are kept in a format that can be produced within 30 calendar days of a request and confirm that you keep the records for five years, or as long as required by the AML/ATF legislation.

¹⁷⁰ FINTRAC *Assessment manual*, March 21, 2022

- Interview your employees and agents to assess their knowledge of record keeping requirements.

FINTRAC's focus is that while it assesses record keeping, it will focus on ensuring that you accurately record information that identifies persons and entities that conduct or direct transactions.

4.4 Submit reports to FINTRAC

The purpose of the reporting obligation is to facilitate FINTRAC's financial analysis and disclosure of information to designated law enforcement agencies and security agencies when it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or threats to the security of Canada.

All reports are important but STRs are extremely valuable to FINTRAC in their analysis. Every effort should be made by accountants and accounting firms to understand the requirement in reporting STRs, as well as all other reportable transactions, to assist FINTRAC in combatting ML/TF. The four reports accountants and accounting firms must submit to FINTRAC within prescribed timelines as outlined in the table below are:

1. suspicious transaction report (STR) - see Chapter 9
2. Terrorist Property Report (TPR) - see Chapters 11 and 29
3. large cash transaction report (LCTR) - see Chapter 10
4. Large Virtual Currency Transaction Report (LVCTR) - see Chapter 10

Table 4 – Report type, method of reporting and timeline

Report type	Method	Timeline	How long must you keep a copy of the report sent to FINTRAC?
STR	Electronic	As soon as practicable ¹⁷¹	At least five years after the day the STR was submitted ¹⁷²
TPR	Paper (mail) or fax only ¹⁷³	Immediately ¹⁷⁴	At least five years after the day the TPR was submitted
LCTR	Electronic	Within 15 calendar days after the transaction ¹⁷⁵	At least five years from the date the LCTR was created
LVCTR	Electronic	Within five working days after the day on which you receive the amount ¹⁷⁶	At least five years from the date the LVCTR was created

All reports to FINTRAC: A report, other than a Terrorist Property Report, must be sent to FINTRAC electronically if you have the technical capabilities to do so¹⁷⁷ or on in paper format if you do not have the technical capabilities to do so. In all cases you must follow FINTRAC’s guidelines for reporting.¹⁷⁸

171 PCMLTFSTRR subsection 9(2)

172 PCMLTFSTRR subsection 12.1(1)

173 FINTRAC, *Reporting terrorist property to FINTRAC*, November 19, 2021

174 PCMLTFSTRR subsection 10(2)

175 PCMLTFR subsection 132(3)

176 PCMLTFR subsection 132(2)

177 PCMLTFR subsection 131(1)

178 PCMLTFR subsection 131(2)

LCTRs and LVCTRs: You should note that while the items in the LCTR and LVCTR are described in the singular, you must report all known information that falls within an item¹⁷⁹ in that report.

When reporting a LCTR or a LVCTR, you must apply what is called the 24-hour rule. The 24-hour rule is the requirement to aggregate multiple transactions when they total \$10,000 or more within a consecutive 24-hour window and the transactions are:

- conducted by the same person or entity
- conducted on behalf of the same person or entity (third-party), or
- for the same beneficiary (person or entity).¹⁸⁰

More information on the 24-hour rule is explained in Section 10.1 of this guide.

TPRs: You must submit TPRs to FINTRAC electronically **by fax** if you have the technical capability to do so. If you do not have the capability to submit by fax, you must send the report by mail.¹⁸¹

FINTRAC's TPR form can be printed from the reporting forms web page¹⁸² or you can request a form to be faxed or mailed to you by calling FINTRAC at 1-866-346-8722.

More information on a TPR, its filing and a copy of the form to FINTRAC is available respectively in Chapters 11 and 29.

4.4.1 FINTRAC examination

For a complete description of FINTRAC's methods for verifying compliance with financial transaction reporting requirements accountants and accounting firms should refer directly to FINTRAC's assessment manual.¹⁸³ What follows is an overview of key areas of examination by FINTRAC for each of the four financial transaction reports for which you are accountable.

179 PCMLTFR subsection 131(3)

180 FINTRAC, *Transaction reporting guidance: the 24-hour rule*, May 4, 2021

181 PCMLTFSTRR section 12

182 FINTRAC, *Reporting forms (paper reporting)*, July 23, 2021

183 FINTRAC *Assessment manual*, March 21, 2022

FINTRAC examination of your financial transaction reporting requirements

FINTRAC may:

- review your policies and procedures to confirm that they provide enough guidance for your employees or agents to meet the reporting requirements
- review your client records, records of transactions and submitted reports to confirm that you adequately apply your policies and procedures
- interview your employees and agents to assess their knowledge of the reporting requirements

FINTRAC will focus on confirming that you have sound policies, procedures, processes and controls in place to adequately meet the following requirements to submit:

- financial transaction reports to FINTRAC (when required)
- the reports on time
- complete and accurate reports

Areas of examination for all four reports

- reviewing changes in your reporting behaviour (increase/decrease in reporting, etc.)
- ensuring that you resubmit the reports FINTRAC rejected for technical errors
- ensuring past reporting issues have been fixed
- ensuring you report on transactions handled by your agents (if applicable)
- ensuring your reports are complete and accurate
- ensuring that your third-party service provider reports correctly (if applicable)
- ensuring that you are sending reports on time

For large cash transaction reports (LCTRs) and Large Virtual Currency Transactions Reports (LVCTRs)

- confirming you are submitting LCTRs and LVCTRs
- confirming you are correctly applying the 24-hour rule to LCTRs and LVCTRs
- confirming that the exception for reporting cash received from financial entities or public bodies is applied to financial entities and public bodies that meet the definition

For suspicious transaction reports (STRs)

- reviewing your policies and procedures on how you monitor activities and transactions
- reviewing your monitoring rules
- reviewing unusual transactions
- reviewing your high-risk areas
- identifying the consistent use of indicators
- reviewing transactions for money laundering and terrorist activity financing indicators
- reviewing how you use publicly available information
- reviewing how you process information from credible sources
- verifying variances in actual versus expected transactional behaviour
- reviewing your client records of transactions for unusual patterns or connections
- reviewing your refunds, cancellations and overpayments
- reviewing how you end relationships with clients and agents

For Terrorist Property Report (TPR)

- reviewing your correspondence with authorities (e.g., CSIS and RCMP)
- confirming the steps you take to determine whether your business possesses or controls the property of a terrorist, terrorist group or listed person, and submit a TPR

4.5 Ministerial directives and transaction limitations/prohibitions

Under Part 1.1 of the PCMLTFA, the Minister of Finance may:¹⁸⁴

- issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities
- recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities

184 FINTRAC, *Ministerial directives and transaction restrictions*, October 28, 2020

4.5.1 Ministerial directives

Ministerial directives are issued in special circumstances by the Minister of Finance under the authority of AML/ATF legislation.¹⁸⁵ A current listing of directives in force can be found on FINTRAC's website.¹⁸⁶

Currently, the only directive applicable to all reporting entities including Accountants and Accounting Firms relates to the Democratic People's Republic of Korea (DPRK).

The ministerial directive pertaining to the Democratic People's Republic of Korea (DPRK) was issued in response to a public statement from the Financial Action Task Force (FATF) on November 3, 2017. In its statement, the FATF expressed its particular and exceptional concerns about North Korea's failure to address the significant deficiencies in its anti-money laundering and combatting the financing of terrorism (AML/CFT) regime and the serious threat this poses to the integrity of the international financial system. The FATF reaffirmed the call on its members to apply effective preventive measures to protect their financial sectors from such risks.

Each directive includes an outline of countermeasures that are limited to the same activities for which reporting entities already have obligations. The countermeasures will enhance or add to these obligations.

Directives specify the date they come into force and will remain in force until officially revoked, suspended or amended. Directives will be reviewed at least every three years from the day they take effect.

This ministerial directive requires that all transactions to and from North Korea be treated as high risk, regardless of the amounts of the transactions.

In addition, FINTRAC's expectation is that you implement specific measures to mitigate the risk posed by these transactions and document the measures taken. When conducting these transactions, regardless of the transaction amounts, the measures you must take to mitigate the risk could include:

- keeping a record of all transactions to and from North Korea, regardless of the amount. This record must include details such as the client's name and address, the amount, currency, date and type of transaction. If the client is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the client is an entity, the nature of their principal business. If the transaction is an electronic

¹⁸⁵ PCMLTFA subsection 11.42(1)

¹⁸⁶ FINTRAC, *Ministerial directives and transaction restrictions*, July 9, 2015

funds transfer, you must record the ordering client and the beneficiary client as well as their addresses, the amount, currency and date of transaction. If the ordering client is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the ordering client is an entity, the nature of their principal business. These details must specify whether funds are coming from, or destined to North Korea.

- identifying clients for all transactions and ensuring that the information you have about the identity of these clients are up to date
- knowing your client, including asking for the:
 - source of the funds
 - purpose of transactions
 - beneficial ownership (if the client is an entity)
- conducting enhanced ongoing monitoring of the client and/or the business relationship and/or the account involved in the transaction
- keeping records of all of the above actions
- reporting suspicious transactions (if applicable)

Policies and procedures should already include general information on how your organization becomes aware of ministerial directives issued by the Minister of Finance as well as identify what you will do in response. Once a directive has been issued, you are expected to take steps to meet the requirements of each directive. In response to this directive, FINTRAC expects you to include the fact that transactions to and from North Korea are high risk as part of your documented risk assessment of clients and business activities.

4.5.2 Transaction limitations/prohibitions

Regulations may be created, on recommendation by the Minister of Finance in consultation with the Minister of Foreign Affairs, to imposing a limitation or a prohibition on any person or entity referred to in section 5 of the PCMLTFA (this includes accountants and accounting firms), with respect to:

- a. entering into, undertaking or facilitating, directly or indirectly, any financial transaction, or any financial transaction within a class of financial transactions, originating from or bound for any foreign state or foreign entity

- b. prescribing terms and conditions with respect to a limitation or prohibition referred to in paragraph (a)
- c. excluding any transaction or any class of transactions from a limitation or prohibition imposed under paragraph (a)

The authority to recommend new regulations to restrict certain transactions is intended to be used in the most serious of cases. The Minister of Finance must consult the Minister of Foreign Affairs before recommending regulations to the Governor-in-Council. These regulations will be published in the Canada Gazette and will be prepared on a case-by-case basis. Accountants and accounting firms should remain vigilant for the potential introduction of such regulations in the future by subscribing to FINTRAC's email list.¹⁸⁷

4.5.3 FINTRAC advisories about financial transactions related to countries identified by the Financial Action Task force (FATF)

FINTRAC publishes advisories to reporting entities from the Financial Action Task Force (FATF) when that organization issues a statement on high-risk jurisdictions subject to a call for action and a statement on jurisdictions under increased monitoring. These statements are updated and released following every Plenary. As noted earlier, accountants and accounting firms should consider subscribing to FINTRAC's email list¹⁸⁸ to ensure that your policies and procedures are kept up to date with the advisories and that your training program also reflects any advisories (when applicable).

4.5.4 FINTRAC examination

FINTRAC may include compliance with ministerial directives (and transaction limitations/prohibitions) as an area of review in any desk review or onsite examination.¹⁸⁹

¹⁸⁷ FINTRAC, *FINTRAC mailing list*, August 16, 2019

¹⁸⁸ Ibid

¹⁸⁹ FINTRAC, *Assessment manual*, March 21, 2022

FINTRAC examination of ministerial directives (and transaction limitations/prohibitions)

Since the instructions provided in each ministerial directive (and any transaction limitation/prohibition)¹⁹⁰ will vary and, as such, FINTRAC's assessment will focus on the essence of the directive. FINTRAC may:

- review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the ministerial directive (and any transaction limitation/prohibition) requirements
- verify that your policies and procedures clarify what ministerial directives (and any transaction limitations/prohibitions) are and where they can be found. FINTRAC may also look to see whether your policies and procedures indicate how often you should check for new, updated or amended directives (and transaction limitations/prohibitions); who should be informed when a directive (and transaction limitation/prohibition) is applicable to your business; and what steps to take to make sure the directive (transaction limitation/prohibition) is being followed
- review your client records and records of transactions to confirm that you put the policies and procedures into practice
- verify that you have taken action when directives (and transaction limitations/prohibitions) are applicable through the review of your client records and records of transactions. These records may include:
 - the verification of the identity of a person or an entity
 - the exercise of customer due diligence including ascertaining the source of funds of a financial transaction, the purpose of a financial transaction or the beneficial ownership or control of an entity
 - monitoring financial transactions for an account
 - keeping records
 - reporting financial transactions to FINTRAC
 - complying with other requirements of the PCMLTFA and associated regulations
- interview your employees and agents to assess their knowledge of the requirements relating to ministerial directives (and any transaction limitations/prohibitions)
- verify that your business follows the directives (and transaction limitations/prohibitions)

¹⁹⁰ Currently no regulations prohibiting or limiting financial transactions have yet been created or are in force, however Accountants and Accounting Firms should check periodically for the introduction of such regulations.

When you conduct business in a foreign jurisdiction or with a foreign entity named in a ministerial directive (and a transaction limitation/prohibition), FINTRAC may:

- verify that your risk assessment considers the parameters of the ministerial directive (and a transaction limitation/prohibition)
- verify that you apply the processes that you have in place to manage high-risk transactions associated with ministerial directives (and a transaction limitation/prohibition), including monitoring the transactions more frequently, applying special measures and submitting suspicious transaction reports when required

FINTRAC will focus on determining whether you are adequately implementing ministerial directives (and transaction limitations/prohibitions).

It is recommended that accountants and accounting firms keep watch on any new ministerial directives or transaction limitations/prohibitions issued by the Minister or the Government.

4.6 Exceptions

The AML/ATF legislation provides for general and specific exemptions to the verification of client identity or the existence of an entity, third-party determination, record keeping and reporting. Listed in this section are the general exceptions.

Specific exceptions are described in each of the Chapters referencing the “Special Events” and in Chapters 23 and 24.

4.6.1 Record keeping exceptions

Record keeping obligations are exempted under certain conditions. There are three general exceptions. Under the AML/ATF legislation the first exception does not require the accountant or accounting firm to complete a large cash transaction record, a Large Virtual Currency Transaction Record or a receipt of funds record if the cash, virtual currency or funds are received from a financial entity, a public body or from a person who is acting on behalf of a client that is a financial entity or public body.

The second general exception in the AML/ATF legislation allows an accountant or an accounting firm that is required to keep a record to **not** include information in that record that is readily obtainable from other records that they are required to keep under the AML/ATF Legislation.¹⁹¹ This means that if you keep the required information and can produce it during a FINTRAC examination you do not need to create a new record to meet your obligations.

The third exception is that there is no requirement to keep a receipt of funds record if the funds are received from a public body, a very large corporation or trust, or a subsidiary of those entities, if the financial statements of the subsidiary are consolidated with those of the public body, or very large corporation or trust.

For example, if an accountant or accounting firm properly fills out a Suspicious Transaction Report and keeps a copy as required, they would not need to capture similar information required in a receipt of funds record, as long the records are kept in a manner in which they can be provided to FINTRAC within 30 days after the day on which a request is made to examine them.¹⁹² For instance, the name and address of the person or entity from whom the funds are received, the exchange rate, the currency, etc. is information required for both the receipt of funds record and the Suspicious Transaction Report. This means that if the required information is kept and can be produced during a FINTRAC examination there is no need to create a new record to meet the obligations. An accountant or accounting firm may choose to maintain the information required in a receipt of funds record as part of its regular records (on paper or electronically in order that a paper copy can be readily produced from it).

The critical point to remember is to be able to provide all the required records to FINTRAC within the required timeframe upon request. FINTRAC's examination focus for record keeping is on ensuring that "you accurately record information that identifies individuals and entities that open or control accounts and conduct or direct transactions."

191 PCMLTFR section 153

192 PCMLTFR section 149

When you receive virtual currency as compensation for the validation of a transaction that is recorded in a distributed ledger or you receive a nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information, you do not need to keep a large virtual currency transaction record.

You are not required to keep records when you undertake other non-triggering activities such as audits, review or compilation engagements.

4.6.2 Reporting exceptions

The AML/ATF legislation does not require the accountant or accounting firm to submit to FINTRAC a large cash transaction report or a Large Virtual Currency Transaction Report when funds are received from a financial entity or public body or from a person who is acting on behalf of a client that is a financial entity or public body.

An exception to reporting electronically, and by paper format only, exists under the AML/ATF legislation if the accountant or accounting firm does not have the technical capability to do so.

4.7 Table summarizing what to do in eight special events when engaged in triggering activities

In this guide, a transaction-related task is defined as keeping a prescribed record, submitting a report to FINTRAC and keeping a copy of that report. There are 19 transaction-related tasks listed in Column A of Table 5 (below). Fifteen tasks are requirements to keep records or copies of reports while four of the tasks (shaded in blue) are the reports you must submit to FINTRAC when the “special event” calls for it. One task requires you to contact the RCMP and CSIS. Eight special events are listed horizontally in columns 1 to 8. The special events or scenarios you may encounter as an accountant or accounting firm are:

1. the receipt of less than C\$3,000 in funds
2. the receipt of C\$3,000 or more in funds¹⁹³
3. the receipt of C\$10,000 or more in cash
4. the receipt of C\$10,000 or more in virtual currency¹⁹⁴

¹⁹³ See PCMLTFR section 125 and Policy Interpretation PI-4542 in Section 20.3. If a transaction is conducted in a foreign currency or virtual currency, the amount of the transaction shall be converted into Canadian dollars using (a) the exchange rate that is published by the Bank of Canada for that foreign currency or virtual currency and that is in effect at the time of the transaction; or (b) if no exchange rate is published by the Bank of Canada for that foreign currency or virtual currency, the exchange rate that the person or entity would use in the ordinary course of business at the time of the transaction.

¹⁹⁴ See Section 10.3

5. the receipt of C\$100,000 or more in cash from a politically exposed person, their family members, or close associates¹⁹⁵
6. the receipt of C\$100,000 or more in virtual currency from a politically exposed person, their family members, or close associates
7. reasonable grounds to suspect money laundering or terrorist financing
8. knowledge of a terrorist group or belief of a listed person property

When one or more of these eight special events arise, the transaction-related tasks noted by a dot (•) must be completed.

Example 1

Being engaged in a triggering activity by itself does not trigger any required transaction-related tasks.¹⁹⁶ For example, the AML/ATF legislation does not require client identification when in receipt of less than \$3,000. Therefore, if you receive C\$2,999 you would be obliged to have a compliance program, but not required to engage in any transaction-related task such as keeping a receipt of funds record and keeping a record of the identity/existence of the client unless another special event occurs at the same time such as a suspicious transaction (column 7) or knowledge of property belonging to a terrorist (column 8).

Example 2

If you encounter special event 2, receiving funds of C\$3,000 or more, five transaction-related tasks must be considered. Two are mandatory such as 1) keep a receipt of funds record and 2) keep record of verification of the identity of the person, the identity and existence of the corporation or entity other than a corporation. The three others listed in column A must be completed to comply with the AML/ATF legislation, if applicable. For instance, if you have established a business relationship with the client, you would be required to 3) keep a business relationship record, 4) keep an ongoing relationship record, and 5) keep record of reasonable measures to confirm the accuracy of beneficial ownership information (if applicable).¹⁹⁷ You would of course be obliged to maintain a compliance program as an already-triggered obligation.

¹⁹⁵ See Section 10.9

¹⁹⁶ Notwithstanding, engaging in any triggering activity gives rise to the obligation to implement and maintain a compliance program.

¹⁹⁷ An explanation of when a business relationship is established is provided in Section 7.2.

Example 3

In combination with any one or more of special events 1,2,3,4,5 and 6 you may also encounter special event 7 suspicious transaction and 8 knowledge of terrorists, terrorist group or belief of a listed person.” If special events 7 or 8 occur, you must complete a suspicious transaction report (STR) or a Terrorist Property Report (TPR) in addition to any required or “if applicable” transaction-related tasks indicated in Table 5 for any of the concurrent special events 1 to 6.

Example 4

In another example using special event 3, if you are receiving C\$10,000 or more in cash from your client or on behalf of the client, you must complete or consider completing all the tasks associated with that special event (i.e., tasks 1 to 10). In addition to your obligation in task 10 to submit a large cash transaction report (LCTR) to FINTRAC, you must submit a suspicious transaction report (STR) to FINTRAC, if you also concurrently have reasonable grounds to suspect a transaction or attempted transaction (event 7). You will therefore submit two different reports to FINTRAC, a LCTR and a STR.

You do not need to create the separate *records* listed in column A, as long as you can produce the records to FINTRAC, upon their request, from your existing system within 30 days after the day of that request.¹⁹⁸

¹⁹⁸ PCMLTFR section 149: Every record that is required to be kept under these regulations shall be kept in such a way that it can be provided to an authorized person within 30 days after the day on which a request is made to examine it under section 62 of the Act.

Table 5

COLUMN A 8 SPECIAL EVENTS If one or a combination of special events on the right occurs, then you must undertake the tasks listed below and consider taking those tasks where noted “if applicable.”	(1) Receiving funds of less than C\$3,000	(2) Receiving funds of C\$3,000 or more	(3) Receiving C\$10,000 or more in cash	(4) Receiving C\$10,000 or more in virtual currency	(5) Receiving C\$100,000 or more in cash	(6) Receiving C\$100,000 or more in virtual currency	(7) Suspicious transaction	(8) Knowledge of terrorists, terrorist group/ belief of a listed person
TASKS								
1. Keep receipt of funds record		•	•		•			
2. Keep record of verification of the identity of the person, the identity and existence of the corporation or entity other than a corporation		•	•	•	•	•	•	•
3. Keep business relationship record ¹⁹⁹ (if applicable)		•	•	•	•	•		
4. Keep ongoing business relationship record (if applicable)		•	•	•	•	•		

199 See PCMLTFR paragraph 4.1(b). An accountant or accounting firm enters into a business relationship the second time they are required to verify the identity of the client.

COLUMN A 8 SPECIAL EVENTS If one or a combi- nation of special events on the right occurs, then you must undertake the tasks listed below and consider taking those tasks where noted “if applica- ble.”	(1) Receiving funds of less than C\$3,000	(2) Receiving funds of C\$3,000 or more	(3) Receiving C\$10,000 or more in cash	(4) Receiving C\$10,000 or more in virtual currency	(5) Receiving C\$100,000 or more in cash	(6) Receiving C\$100,000 or more in virtual currency	(7) Suspi-cious transac-tion	(8) Knowl-edge of terrorists, terrorist group/ belief of a listed person
TASKS								
5. Keep record of reasonable measures to confirm the accuracy of beneficial ownership information (if applicable)		•	•	•	•	•		
6. Keep record of third-party determination for large cash/ Large Virtual Currency Transaction			•	•	•	•		
7. Keep record of grounds to suspect third-party involvement for large cash/Large Virtual Currency Transactions			•	•	•	•		
8. Keep large cash transaction record			•		•			

COLUMN A 8 SPECIAL EVENTS If one or a combination of special events on the right occurs, then you must undertake the tasks listed below and consider taking those tasks where noted “if applicable.”	(1) Receiving funds of less than C\$3,000	(2) Receiving funds of C\$3,000 or more	(3) Receiving C\$10,000 or more in cash	(4) Receiving C\$10,000 or more in virtual currency	(5) Receiving C\$100,000 or more in cash	(6) Receiving C\$100,000 or more in virtual currency	(7) Suspicious transaction	(8) Knowledge of terrorists, terrorist group/ belief of a listed person
TASKS								
9. Keep copy of large cash transaction report			•		•			
10. Submit large cash transaction report to FINTRAC			•		•			
11. Keep Large Virtual Currency Transaction Record				•		•		
12. Submit Large Virtual Currency Transaction Report to FINTRAC				•		•		
13. Keep Copy of Large Virtual Currency Transaction Report (LVCTR)				•		•		

COLUMN A 8 SPECIAL EVENTS If one or a combination of special events on the right occurs, then you must undertake the tasks listed below and consider taking those tasks where noted “if applicable.”	(1) Receiving funds of less than C\$3,000	(2) Receiving funds of C\$3,000 or more	(3) Receiving C\$10,000 or more in cash	(4) Receiving C\$10,000 or more in virtual currency	(5) Receiving C\$100,000 or more in cash	(6) Receiving C\$100,000 or more in virtual currency	(7) Suspicious transaction	(8) Knowledge of terrorists, terrorist group/ belief of a listed person
TASKS								
14. Keep PEP, HIO, family and close associate record when receiving \$100,000 or more in cash or virtual currency					•	•		
15. Submit suspicious transaction report to FINTRAC							•	
16. Keep copy of suspicious transaction report							•	
17. Submit Terrorist Property Report (TPR) to FINTRAC								•
18. Keep copy of TPR								•
19. Contact RCMP and CSIS ²⁰⁰ (if TPR submitted)								•

²⁰⁰Information on knowledge of terrorist property must be provided to the RCMP and CSIS immediately.

CHAPTER 5

About money laundering and terrorist financing

5.1 Money laundering

Money laundering methods are often described in three stages: placement, layering and integration. A money launderer's first problem where, for example, the proceeds of crime originate from drug trafficking, is typically placing cash into the financial system. The placement stage attracts the most attention and is the one at which most money laundering laws, and risk mitigation tools are directed, and is arguably one of the hardest stages to achieve in such a scenario. Even if just this one stage is accomplished, the dirty money has been laundered – since the proceeds of crime have been converted. Placement is so critical to money laundering because once nefariously generated funds are in the system, it becomes difficult to distinguish a good dollar from a bad dollar. Placement is sometimes accomplished by simply depositing illicitly generated funds at a financial institution, while others involve converting cash into commodities like gold and diamonds before selling them into the financial system.

More sophisticated schemes also try to create further distance and obscurity between that original transaction and the ultimate use of the money – ideally severing the audit trail, a process called layering. Layering might involve changing the domicile of money or transferring it in ways that obscures the origin or destination of the funds. Integration is commonly known as the final stage of money laundering – it is the stage during which the proceeds of crime are used to buy assets or pay for further criminal operations. For a money launderer, it is ideal that the assets and payments funded by criminal activities have an alternative legitimate explanation for their origin.

The methods and techniques employed at any of those stages vary in complexity and sophistication and will depend on the jurisdiction, the origins and amount of money that needs to be cleaned. A report issued by the Egmont Group,²⁰¹ a worldwide association of Financial Intelligence Units, suggests five general categories of means by which money is laundered (known as typologies): concealment within business structures; misuse of legitimate businesses; use of false identities, documents, or straw men; exploiting international jurisdictional issues; and the use of anonymous asset types. A report by the FATF titled *Guidance for A Risk-Based Approach - Accounting Profession*²⁰² provides insight into the vulnerabilities to ML/TF of accountants.

5.1.1 Concealment within business structures

Money laundering schemes can involve concealing illicit proceeds of crime within the structure of an existing business owned or controlled by the criminal organization. The funds can be intermingled with legitimate transactions of the business and moved throughout the financial system. Detecting this type of activity is difficult as it may take great amounts of analysis to distinguish between legitimate business transactions and those above and beyond which would be from criminal activities. False invoices and receipts can be utilized to demonstrate to their financial institution that the transactions have in fact “occurred.” However, the funds being deposited are in fact proceeds of crime disguised as legitimate business profits.

5.1.2 Misuse of legitimate businesses

A similar scheme is through legitimate businesses which are not controlled by the criminal organization. One advantage over the previous scheme is that this method provides additional separation for the criminal organization as the criminal funds would be linked to the legitimate business and not the criminals misusing the business. For instance, illicit funds may be deposited with a financial institution and transferred to an account held at a foreign financial institution.

5.1.3 Use of false identities, documents or straw men

False identities, documents and straw men are another common method utilized to launder proceeds of crime. This involves separating the assets from a criminal and associating the funds with an individual who had no

201 Joint Financial Intelligence Unit (JFIU), *FIU's in Action: 100 cases from the Egmont Group*
202 FATF, *Guidance for a risk-based approach: Accounting Profession*, June 2019

involvement with the initial criminal activity. For instance, false documents and identities can be used to open bank accounts and create a buffer between the criminal and the illicit funds. Even if the criminal is prosecuted and has all assets under their name seized, the assets held under a false identity will be available.

5.1.4 Exploiting international jurisdictional issues

On a larger scale, international jurisdictions are exploited for the benefit of laundering money. Criminals will take advantage of differing legislation in foreign jurisdictions to successfully launder illicit proceeds of crime. For instance, identification requirements, disclosure requirements, company formation laws and secrecy laws all provide avenues that are exploited for the benefit of disguising and laundering funds. In favourable jurisdictions, criminals can open bank accounts, form corporations and send funds with ease and secrecy and, therefore, distort the true source and ownership of the illicit funds.

5.1.5 Use of anonymous asset types

Similarly, the use of anonymous asset types allows criminals to separate the ownership of the assets from themselves and any law enforcement actions related to those assets. Cash, jewellery and precious metals are all anonymous asset types favoured by criminals. This explains the prevalence of conducting drug trafficking in cash as opposed to other payment methods which can be traced back to the criminal.

5.2 Terrorist financing

A terrorist financing offence means an offence under section 83.02, 83.03 or 83.04 of the Criminal Code or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act. A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

The offences are varied and specific to terrorist activities, as defined in the Criminal Code, but can be summarized as intentionally, directly or indirectly “...causing death or serious bodily harm to a civilian or to any other person

not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act.” It also includes providing, making available, property or services for terrorist purposes and using or possessing property for terrorist purposes.

Terrorism remains a constant threat in Canada. At the time of writing this guide, the threat level of terrorism in Canada²⁰³ was assessed as medium, meaning that a violent act of terrorism could occur. Internationally referred to as “gatekeepers,” accountants and accounting firms have been included in the effort to prevent terrorist activity when they are engaged in triggering activities by filing reports to FINTRAC and contacting the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) in certain circumstances (see Section 9.1.1 and Chapter 11). Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to intimidate a population or compel a government to do something. This is done by intentionally killing, seriously harming or endangering an individual or causing substantial property damage that is likely to seriously harm people. It can also be done by seriously interfering with or disrupting essential services, facilities or systems.

Terrorist activity is undertaken for political, religious or ideological purposes. This does not mean that an expression of political, religious or ideological beliefs alone is a terrorist activity, unless it is part of a larger conduct that meets the definition explained above.

Terrorists need financial support to carry out terrorist activities and achieve their goals. In this respect, there is little difference between terrorists and other criminals in their use of the financial system. A successful terrorist group, much like a criminal organization, is one that is able to build and maintain an effective financial infrastructure. For this, it must develop sources of funding and means of obscuring the links between those sources and the activities the funds support. It needs to find a way to make sure that the funds are available and can be used to get whatever goods or services are needed to commit terrorist acts. The sums needed to mount terrorist attacks are not always large and the associated transactions are not necessarily complex.

203 Government of Canada, [Canada's National Terrorism Threat Level](#)

5.3 Indicators of money laundering and terrorist financing

In its guidance related to STRs, FINTRAC provides a number of indicators about which accountants and accounting firms should be vigilant.²⁰⁴ The presence of an indicator is one factor which may lead to the consideration of an STR, but by itself is not definitive. Facts related to the transaction or the client's financial history, and contextual information about the client, the transaction(s) and historical behaviour will assist in determining whether there are reasonable grounds to suspect the transactions are relevant to a money laundering or terrorist financing offence.

FINTRAC has identified 13 categories of indicators including one that is specific to accountants and accounting firms. All indicators in these 13 are listed in Chapter 30 – Appendix P. FINTRAC has also published “Indicators of ML/TF Related to Virtual Currencies”. These are listed in Chapter 31 – Appendix Q. Every accountant and accounting firm should familiarize themselves with the full list of suspicious indicators, as amended from time to time by FINTRAC, as part of their ongoing training program. Below are the 13 categories of indicators followed by examples of ML/TF indicators specific to accountants and accounting firms.

The 13 categories of money laundering ML/TF indicators organized by topic found in the FINTRAC guidance are:

1. ML/TF indicators related to identifying the person or entity
2. ML/TF indicators related to client behaviour
3. ML/TF indicators surrounding the financial transactions in relation to the person/entity profile
4. ML/TF indicators related to products and services
5. ML/TF indicators related to change in account activity
6. ML/TF indicators based on atypical transactional activity
7. ML/TF indicators related to transactions structured below the reporting or identification requirements
8. ML/TF indicators involving wire transfers (including electronic funds transfers)
9. ML/TF indicators related to transactions that involve non-Canadian jurisdictions
10. ML/TF indicators related to use of other parties
11. Indicators specifically related to terrorist financing

²⁰⁴FINTRAC, *Money laundering and terrorist financing indicators - Accountants*, June 1, 2021

12. ML/TF indicators specific to accountants
13. ML/TF indicators related to virtual currencies²⁰⁵

Examples of ML/TF indicators specific to accountants and accounting firms are as follows:

- 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

²⁰⁵ Refer to Chapter 31 - Appendix Q - Indicators of ML/TF related to virtual currencies or [related FINTRAC guidance](#).

CHAPTER 6

Implement and maintain a compliance program

The AML/ATF legislation requires that accountants and accounting firms implement and keep an up-to-date program to achieve compliance with required tasks. The compliance program is comprised of six mandatory components:

1. **Appointment of a compliance officer.**²⁰⁶ The compliance officer must be a person who is responsible for implementing the compliance program.
2. **Development and application of written compliance policies and procedures.**²⁰⁷ These must be kept up to date and, in the case of an accounting firm (entity), they are approved by a senior officer.
3. **An assessment and documentation of the risk of ML/TF.**²⁰⁸ The risk assessment must take into account your clients and business relationships, your products, services and delivery channels, the geographic location of your activities and any other relevant factor,

²⁰⁶ Compliance officer means the individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. This definition can be found in [FINTRAC's glossary](#) and in Section 3.5.1 of this guide.

²⁰⁷ Compliance policies and procedures means the written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated regulations and the corresponding processes and controls you put in place to address your obligations. This definition can be found in [FINTRAC's glossary](#) and in Section 3.5.1 of this guide.

²⁰⁸ Risk assessment means the review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. This definition can be found in [FINTRAC's glossary](#) and in Section 3.5.1 of this guide.

4. **Development and maintenance of a written ongoing training program.**²⁰⁹
If the accountant or accounting firm has employees, agents or mandataries²¹⁰ or other persons who are authorized to act on their behalf, they must develop and maintain a written, ongoing compliance training program for those employees, agents or mandataries or other persons.
5. **Instituting and documenting a training plan.** Instituting and documenting a plan for the ongoing compliance training program and delivering the training (training plan).
6. **A review and test of the effectiveness of the compliance program.** Instituting and documenting a plan for a review of the compliance program for the purpose of testing its effectiveness and carrying out this review every two years at a minimum. (two-year effectiveness review).²¹¹

FINTRAC has indicated that during an examination, it may examine your compliance program and its components.

FINTRAC examination of your compliance program

- FINTRAC has indicated in its assessment manual²¹² that it will verify that you have a well-documented and complete compliance program in place and will assess whether your compliance program is put into practice.
- To do so, FINTRAC will assess your compliance with other requirements, such as client identification and other know your client requirements, reporting requirements and record keeping requirements. FINTRAC may consider deficiencies identified through the assessment of these other requirements to be an indication that one or more of the five elements of your compliance program is not being applied.

²⁰⁹ Training program means a written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated regulations. This definition can be found in [FINTRAC's glossary](#) and in section 3.5.1 of this guide.

²¹⁰ Mandatary means a person who acts, under a mandate or agreement, for another person or entity. This definition can be found in [FINTRAC's glossary](#) and in section 3.5.1 of this guide.

²¹¹ Two-year effectiveness review means a review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment and training program. This definition can be found in [FINTRAC's glossary](#) and in section 3.5.1 of this guide.

²¹² FINTRAC, *Assessment manual*, March 21, 2022

6.1 Appoint a compliance officer

As part of the compliance program, you are required to appoint a person who is responsible for its implementation. The compliance officer has an overall accountability for the compliance program. The person that is appointed in the role of the compliance officer should be adequately qualified, maintain relevant anti-money laundering and counter terrorist financing knowledge and have direct access to individuals who make important decisions about compliance issues or who control the office or firm. The appointment of the compliance officer should be formalized within the organization in a written document and available for review by FINTRAC upon examination. Any changes to that appointment should also be formally documented.

Depending on the size of your office or firm, you could be the appointed compliance officer, or it could be another individual, such as:

- a senior manager, or
- someone from a senior level who has direct access to senior management and the board of directors of your firm

If you are an individual accountant, you can appoint yourself as the compliance officer, or you may choose to appoint another individual to help you implement the compliance program. As a best practice, the appointed compliance officer of a larger firm should not be directly involved in the receipt, transfer or payment of funds, or giving instructions on these triggering activities.

The person that is appointed the role of the compliance officer should:²¹³

- have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes
- have knowledge of your business's functions and structure
- have knowledge of your business sector's ML/TF risks and vulnerabilities as well as ML/TF trends and typologies
- understand your business sector's requirements under the PCMLTFA and associated regulations

As a best practice, your compliance officer should be adequately qualified with appropriate professional qualifications, experience and strong leadership skills.

213 FINTRAC, *Compliance program requirements*, August 4, 2021

An appointed compliance officer may delegate certain duties to other employees. For example, the compliance officer of a large firm may delegate responsibility to an individual in another office or branch. However, the compliance officer remains responsible for the implementation of the compliance program under the AML/ATF legislation and, as a best practice, where such a delegation is made, it should be formalized.

6.1.1 Sample role description of a compliance officer

As a best practice, a job description for the compliance officer should be formalized, describing their authority and position in an organizational chart. The organization's AML/ATF policies and procedures should provide sufficient guidance for the compliance officer to meet the legal requirements. The compliance officer should:

- have the ability to report compliance related issues to and meet with the senior officer²¹⁴ on a regular basis
- ensure that the AML/ATF policies and procedures are kept up to date and that all changes are approved by a senior officer
- ensure that the risk-based training program is documented and tailored to meet the AML/ATF roles and responsibilities of different staff and contractors
- ensure that the effectiveness review of the organization's compliance program will be conducted every two years and reported within 30 days to a senior officer after the completion of the review
- conduct an assessment of the inherent risk of money laundering and terrorist financing on an ongoing basis
- understand and monitor the effectiveness of the technology used to enable AML/ATF compliance to ensure that transactional alerts and regulatory reports generated are accurate, complete and reflect the actual operations of the organization

6.1.2 FINTRAC examination

FINTRAC has indicated that during an examination, it may examine your appointment of a compliance officer.

214 PCMLTFR subsection 1(2) and [FINTRAC guidance glossary](#) - Senior officer is defined as : a) a director of the entity who is one of its full-time employees; (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

FINTRAC examination of the appointment of a compliance officer

In its assessment manual,²¹⁵ FINTRAC indicates that it uses the methods described in this section to assess your compliance with the requirement to appoint a compliance officer who is responsible for implementing your compliance program. FINTRAC will verify that the following criteria have been adequately met: appointment (selection), authority, knowledge and duties. They may:

- review documents that show you have formally appointed a compliance officer. FINTRAC may also review your compliance officer's job description, documents that describe their authority, and an organizational chart. FINTRAC may also review your policies and procedures to confirm that they give your compliance officer enough guidance to meet the legal requirements, that they have direct access to senior management or board of directors and access to information from all business lines (where applicable)
- look at the compliance officer's background and experience, as well as the training you have given them to verify that you have made sure that the officer has enough knowledge of your:
 - business's functions and structure
 - sector's money laundering and terrorist activity financing risks and vulnerabilities, as well as related trends and typologies
 - sector's requirements under the AML/ATF legislation
- interview your employees to confirm that the compliance officer has direct access to the individuals who make important decisions about compliance issues or who control the firm

FINTRAC's focus will be on verifying that the compliance officer is fulfilling their duties to implement a sound compliance program. To make this determination, FINTRAC assesses whether the areas of your compliance program that they examined are adequately put into practice.

215 FINTRAC, *Assessment manual*, March 21, 2022

6.2 Develop and apply written compliance policies and procedures

FINTRAC has provided guidance on the requirements related to your compliance policies and procedures.²¹⁶ Accountants and accounting firms are required to have policies and procedures that are:

- written and in a form/format that is accessible to its intended audience
- kept up to date (including changes to legislation or your internal processes, as well as any other changes that would require an update)
- approved by a senior officer, if you are an entity²¹⁷

Your compliance policies and procedures should also include the processes and controls you have put in place to meet your requirements, including:

- when the obligation is triggered
- the information that must be reported, recorded or considered
- the procedures you created to ensure that you fulfill a requirement
- the timelines associated with your requirements and methods of reporting (if applicable)

Your policies and procedures must also describe the steps you will take for all the obligations that require you to take reasonable measures.²¹⁸ For example, when you are required to take reasonable measures to obtain information to include in a report, your policies and procedures must describe the steps you will take, which could include asking the client.

The level of detail in your compliance policies and procedures will depend on your business's size, structure and complexity, and degree of exposure to ML/TF risks.

In essence, your compliance policies and procedures should document applicable legislative requirements and the organization's procedures to satisfy those requirements. Procedures should also include those that were developed as part of the risk-based approach.

The compliance policies and procedures should be approved by a senior officer and kept up to date, taking into consideration:

- changes to AML/ATF legislative requirements

²¹⁶ FINTRAC, *Compliance program requirements*, August 4, 2021

²¹⁷ Entity means a body corporate, a trust, a partnership, a fund or an unincorporated association or organization as defined in the PCMLTFA subsection 2(1), in FINTRAC's guidance glossary and in this guide at Section 3.5.1

²¹⁸ As defined in *FINTRAC's glossary*, reasonable measures means steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following: asking the client, conducting open-source searches, retrieving information already available, including information held in non-digital formats, or consulting commercially available information.

- changes to internal processes and procedures
- changes in products and services that have an effect on AML/ATF requirements (for example, new services that are triggering activities)
- the development and implementation of new technologies
- changes in organizational structures that could affect reporting procedures

Considering the parameters and organization of the AML/ATF legislation in respect to accountants and accounting firms, it is expected that, at a minimum, the policies listed below would form part of an accountant or accounting firm's compliance program.

6.2.1 General policies

Here are some general policies you may wish to consider as part of your compliance program.

- “We will identify all triggering activities as they occur within our organization.”
- “We will define the triggering activities along with explanations of where within the organization such activities are being conducted.”

6.2.1.1 Compliance program

- “We will appoint a qualified compliance officer that meets the requirements of FINTRAC's Guidance.”
- “We will develop and implement a compliance program that includes the requirements for a risk assessment, an ongoing compliance training program and plan and a two-year effectiveness review and plan, consisting of a review of our policies and procedures, risk assessment and ongoing training program and plan.”
- “We will subscribe to the Department of Finance Canada's and FINTRAC's news releases to keep up to date on new legislative developments, policies, guidance, ministerial directives, transaction restrictions/prohibitions, typologies and procedures.”
- “We will update our policies and procedures to reflect new AML/ATF legislation requirements, FINTRAC guidance, interpretation notices and policy interpretations as they arise.”

6.2.1.2 *Know your client*

6.2.1.2.1 *Verification of identity and verification of existence*²¹⁹

- “When a large cash or a large virtual currency transaction is conducted, the identity of the conductor will be verified.”
- “Verification of a person’s identity and the verification of an entity’s identity and existence will be conducted using prescribed methods to ensure accuracy of the information.”

Government-issued photo identification method

- “We will describe the processes we follow to determine whether a government-issued photo identification document is authentic, whether the client is present or not, and how we will confirm that it is valid and current.”
- “We will describe the steps we use to confirm that the name and photograph are those of the person.”
- “Our processes will determine that a government-issued photo identification document is authentic, valid and current although the verification step (ensuring that the name and photo match the name and appearance of the person), do not need to happen at the same time.”

Credit file method

- “We will describe the processes we follow to verify a person’s identity using the credit file method and how we will ensure that the information is valid and current.”
- “We will include the steps we will take if the information is not valid and current (for example, search a different credit file, use another method, stop the transaction, etc.).”

Dual-process method

- “We will describe the processes we follow when using the dual-process method to verify a person’s identity and how we will ensure that the information is valid and current.”

Reliance method

- “We will describe the processes we follow when using the reliance method to verify a person’s identity and how we will ensure that the information is valid and current.”

²¹⁹ FINTRAC Guidance on when to [verify the identity of persons and entities](#) and [methods to verify the identity of persons and entities](#).

Using an agent or mandatary to verify the identity of a person

- “We will describe the processes we follow when you rely on an agent or mandatary to verify a person’s identity and how we will ensure that the information is valid and current.”
- “Verification of an entity’s identity will be conducted using prescribed methods to ensure accuracy of the information.”

Confirmation of existence method

- “We will describe the processes we follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how we will ensure that the information is authentic, valid and current.”

Reliance method

- “We will describe the processes we follow when using the reliance method to verify the identity of corporations and other entities and how we will ensure that the information is valid and current.”
- “All clients who are the subject of suspicious transactions will have their identification verified except when doing so would tip off the client that a suspicious report is being sent to FINTRAC.”
- “When a receipt of funds record is created, the client’s identification will be verified and if the individual is acting on behalf of an entity, the entity’s existence will also be verified.”

6.2.1.2.2 *Third-party determination*²²⁰

- “For every large cash and virtual currency transaction, a third-party determination will be made and if there is a third-party connected to the transaction, a record will be kept documenting their details.”

6.2.1.2.3 *Beneficial ownership*

- “The beneficial ownership of all entities being verified will be obtained, retained and recorded as prescribed.”
- “If the beneficial ownership information cannot be obtained, reasonable measures will be taken to verify the identity of the entity’s chief executive officer or the person who performs that function, and special measures will be taken.”

²²⁰ FINTRAC, *Third party determination requirements*, August 4, 2021

6.2.1.2.4 Politically exposed persons, heads of international organizations, family members and close associates

- “If we receive \$100,000 or more, in cash or in virtual currency, from a person we will take reasonable measures to determine whether the person is a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a family member of, or a person who is closely associated with, one of those persons.”
- “If we enter into a business relationship, have a business relationship or detect a fact that constitutes reasonable grounds to suspect that a person with whom we have a business relationship is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization, a family member of one of those persons or a close associate we will take specific reasonable measures as prescribed.”

6.2.1.3 Business relationships and ongoing monitoring²²¹

- “We will determine that we have entered into a business relationship as soon as possible after verifying our client’s identity for the second transaction or activity where we have had the obligation to do so.”
- “As a best practice, we will make a business relationship determination within 30 calendar days of a second transaction or activity.”
- “We will conduct ongoing monitoring of our business relationships to periodically monitor the business relationship and keep an ongoing business relationship record.”

6.2.1.4 Record-keeping²²²

- “All required records will be documented and stored for at least five years.”
- “All records will be stored in such a way that allows for their retrieval within 30 days of notice by FINTRAC.”
- “A receipt of funds record will be kept for every transaction where we accept \$3,000 or more in funds from a client.”
- “A large cash transaction and virtual currency transaction record will be kept for every transaction where we accept \$10,000 or more in cash or virtual currency from a client, whether at one time or within 24 hours.”
- “Copies of official corporate records will be kept for all transactions that require the verification of the existence of a corporation.”
- “A copy of all transaction reports submitted to FINTRAC will be stored on file.”

221 FINTRAC, *Business relationship requirements*, August 4, 2021 and FINTRAC, *Ongoing monitoring requirements*, August 4, 2021.

222 FINTRAC, *Record keeping requirements for accountants*, August 4, 2021

6.2.1.5 *Enhanced measures for high-risk clients*

- “We will take prescribed special (enhanced) measures when dealing with a high-risk client including: taking enhanced measures to verify the identity of persons and entities and verify the existence of entities when they are assessed as high-risk clients, taking enhanced measures to keep client information up to date, taking enhanced measures to keep beneficial ownership information up to date, taking enhanced measures to conduct ongoing monitoring of business relationships for the purposes of detecting transactions that are required to be reported as suspicious transaction reports; and taking any other enhanced measures to mitigate the risks identified.”

6.2.1.6 *Transaction reporting*²²³

- “All large cash transactions will be reported to FINTRAC within 15 calendar days of receipt whether received at one time or within 24 hours.”
- “All large virtual currency transactions will be reported to FINTRAC within five working days after the day on which the amount is received.”
- “All suspicious transactions, whether completed or attempted, will be reported to FINTRAC as soon as practicable.”
- “A listing of all suspicious transaction indicators will be developed and maintained which will lead to reporting.”
- “Any terrorist property will be reported to FINTRAC immediately upon knowing or believing that we are dealing with terrorist or listed person property. CSIS and the RCMP will be contacted immediately.”
- “Our process for submitting Terrorist Property Reports (TPRs) will be described, including our process to identify terrorist property.”
- “Our processes will ensure TPRs are complete and accurate when submitted to FINTRAC, and our compliance training program will ensure our employees, agents or other individuals authorized to act on our behalf are aware of our terrorist property reporting requirements.”²²⁴
- “We will describe measures needed to enable suspicious transaction report (STR) submission to FINTRAC including: screening for and identifying suspicious transactions; assessing the facts and context surrounding the suspicious transaction; linking ML/TF indicators to our assessment of the facts and context; and explaining our grounds for suspicion in an STR, where we articulate how the facts, context and ML/TF indicators allowed us to reach our reasonable grounds for suspicion.”

223 FINTRAC, *Transactions that must be reported*, June 1, 2021

224 FINTRAC, *Reporting terrorist property to FINTRAC*, November 19, 2021

- “After completing the measures that enabled us to determine that we have reasonable grounds to suspect that a financial transaction is related to the commission or attempted commission of an ML/TF offence, we will submit an STR to FINTRAC as soon as practicable.”
- “We will describe how, in situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, as a best practice, we will expedite the submission of our STRs.”
- “We include the time when our 24-hour windows begin and end in our description of the 24-hour rule and we will indicate the times that your 24-hour window begins and ends in a mandatory field when we submit a report to FINTRAC.”

6.2.1.7 Ministerial directives and transaction limitations/prohibitions²²⁵

- “We will keep up to date on all ministerial directives and transaction limitations/prohibitions issued by the Department of Finance and FINTRAC and implement the required measures.”
- “We will keep abreast of FINTRAC advisories.”

6.2.2 Sample list of policies and procedures headings

Policies and procedures need to include all legislative requirements under the AML/ATF legislation and be specific to your organization. The factors below can be used to determine the framework of a complete set of policies and procedures.

- policy statement
 - objective: explains the objective of the policy
 - responsibility: explains who is responsible for the compliance program
 - background (including relevant legislative requirements and guidance): provides a summary of legislation that is applicable to the document
 - policy application: explains to whom the policies are applicable
- procedures
 - responsibilities: explanation of all accountable parties
 - appointment of compliance officer: statement explaining how the appointment is made and who is the current compliance officer
 - procedure application: explains to whom the procedures are applicable
 - foreign currency transaction: explanation of how transactions in a foreign currency will be treated
- compliance operations

²²⁵ FINTRAC, *Ministerial directions and transaction restrictions*, September 27, 2021

- identifying triggering activities: explanation of how these activities will be found in the organization
- receipt of funds of less than \$3,000: explains what is not required
- receipt of funds of \$3,000 or more: explains the record keeping and identity verification steps taken when these occur
- receipt of cash or virtual currency of \$10,000 or more: explains the record keeping, verification of identity and reporting steps taken when these occur
- receipt of cash or virtual currency of \$100,000 or more when a business relationship or a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a family member of, or a person who is closely associated is, or may be, involved: explains the record keeping, verification of identity and reporting steps taken when these occur
- completed and attempted suspicious transactions: explains how these transactions are initially detected and the measures taken when they are detected
- Terrorist Property Reports: explains the process for determining if property is held and the steps taken when a positive match is found
- business relationship establishment and ongoing monitoring explains the concept and what measures are taken to satisfy the requirements
- special measures (enhanced measures): establishes the measures taken and when they would be applicable
- risk-based approach
 - responsibility and application: explains who is accountable for this and how it applies
 - risk assessment: includes the five prescribed factors and classifies all areas into a specific risk category
 - risk mitigation: explains the enhanced measures taken for areas deemed to be high risk
- training program
 - responsibility and application: explains who this applies to and the person/team accountable for this program
 - program content: summarizes the training material, who does the training, how often, etc.
- effectiveness review
 - responsibility and application: explains who is accountable for this program component
 - requirements: explains the methodology and frequency that will apply

6.2.3 FINTRAC examination

FINTRAC has indicated that during an examination, it may examine your policies and procedures.

FINTRAC examination of policies and procedures

In its assessment manual,²²⁶ FINTRAC has indicated that it uses the following methods to assess your compliance with the requirement to develop, document and apply policies and procedures. FINTRAC verifies that your policies and procedures cover the following (if applicable): compliance program requirements, client identification and other know your client requirements, financial transaction reporting requirements, record keeping requirements and ministerial directive and transaction limitation/prohibition requirements.

FINTRAC also verifies that your policies and procedures are adequate, tailored to your business (that is, they take into account the type, nature, size, and complexity of your business) and are designed to control the risks you may face. To conduct this assessment, FINTRAC may:

- review your policies and procedures to confirm that they are written, up to date and, if your business is an entity, approved by a senior officer
- review your policies and procedures to confirm that they provide enough guidance for your employees or agents
- interview your employees and agents to assess their knowledge of your policies and procedures

FINTRAC will focus on ensuring that you are adequately putting the policies and procedures into practice with respect to your obligations, including reporting, client identification, beneficial ownership, third-party determination, politically exposed persons and heads of international organizations, ministerial directives, transaction limitations/prohibitions and special measures for high-risk client requirements, when required.

226 FINTRAC, *Assessment manual*, March 21, 2022

6.3 Assess and document the risk of ML/TF

6.3.1 Accountants' and accounting firms' risk of ML/TF

As a profession, accountants and accounting firms have been included in Canada's AML/ATF legislation since 2000. From some of the Financial Action Task Force's (FATF) earliest typologies reports, professional accountants have been identified globally as “gatekeepers”²²⁷ to the financial system, and intermediaries that are well placed to contribute to combatting money laundering and terrorist financing. In 2019, the FATF²²⁸ described the wide range of services internationally that professional accountants may provide, depending upon their jurisdiction, in public practice to a diverse range of clients, as well as many of the functions that are most susceptible to attract money launderers such as providing financial and tax advice,²²⁹ company and trust formation, buying or selling of property, etc.

As a result, professional accountants play a crucial role in contributing to the integrity of the financial system globally. In Canada, accountants and accounting firms contribute to the safety and security of Canadians by complying with the AML/ATF legislation as required. In 2015, the Department of Finance Canada published a national assessment of inherent risks of money laundering and terrorist financing in Canada. Accountants and accounting firms were assessed as having a medium overall rating of inherent money laundering/terrorist financing vulnerability.

In 2021, the FATF released a report recognizing Canada's progress in strengthening measures to tackle money laundering and terrorist financing, since its original assessment in 2016.²³⁰

6.3.2 Requirement for a risk assessment

Accountants and accounting firms are obligated to include in their compliance program the conduct and documentation of a money laundering and terrorist financing risk assessment, and to adopt measures which mitigate identified risks.

227 FATF, *Report on Money Laundering Typologies 2003-2004*, p. 24, February 26, 2004

228 FATF, *Guidance for A Risk-Based Approach – Accounting Profession*, June 2019

229 Under the AML/ATF legislation, giving instructions is a covered activity when related to other triggering activities and is distinct from giving advice. See FINTRAC *Interpretation Notice No.2*, August 16, 2019.

230 FATF, *Anti-money laundering and counter-terrorist financing measures – Canada, 4th Enhanced Follow-up Report & Technical Compliance Re-Rating*, September 2021

Risk assessment requirements are prescribed at subsection 9.6(2) of the PCMLTFA, and paragraph 156(1)(c) and subsection 156(2) of the PCMLTFR. Those provisions require that accountants and accounting firms assess and document the risk (likelihood and significance) of money laundering or terrorist financing activity occurring in the course of their activities. It must consider the organization's:

- clients and business relationships, including their activity patterns and geographic locations
- products, services, and delivery channels offered
- geographic location(s) of activities where you conduct your activities
- any other relevant factor affecting your business (for example, employee turnover, professional rules and regulations)
- risks from new developments or introduction of new technology you intend to carry out or introduce, before doing so, that may have an impact on your clients, business relationships, products, services or delivery channels, or the geographic location of your activities.²³¹

FINTRAC has published guidance on the risk-based approach to combatting money laundering and terrorist financing²³² to help reporting entities better understand what the risk-based approach is and assist them in taking inventory of their risks relating to products, services and delivery channels, clients and business relationships, geography and other relevant factors. You may wish to consult FINTRAC's guidance to assist in establishing your risk assessment for ML/TF.

The PCMLTFA at subsection 9.6(3) and the PCMLTFR at section 157²³³ require that prescribed special measures be taken for higher risk activities, including developing and applying written policies and procedures for periodic client identification updates, keeping beneficial ownership and business relationship information up to date, ongoing monitoring for the purpose of detecting suspicious transactions, and others that mitigate identified risks.

²³¹ PCMLTFR subsection 156(2). The AML/ATF legislation requires that if you intend to carry out a new development or introduce a new technology that may have an impact on your clients, business relationships, products, services or delivery channels or the geographic location of their activities, you must assess and document the risk before doing so.

²³² FINTRAC, *Risk assessment guidance*, August 4, 2021

²³³ PCMLTFR section 157: The prescribed special measures that are required to be taken by a person or entity referred to in subsection 9.6(1) of the Act for the purposes of subsection 9.6(3) of the Act are the development and application of written policies and procedures for (a) taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity; and (b) taking any other enhanced measure to mitigate the risks, including (i) ensuring, at a frequency appropriate to the level of risk, that client identification information and information collected under section 138 is up to date, and (ii) conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships referred to in section 123.1.

Ultimately, risk assessments should lead to controls designed to make it more difficult for criminal elements to use accountants and accounting firms to launder their illicit proceeds.

The PCMLTFA and associated regulations do not prohibit you from having high-risk activities or high-risk business relationships. However, it is important that if you identify high-risk activities or high-risk business relationships that you document and implement appropriate controls to mitigate these risks and apply prescribed special measures.

6.3.3 Risk assessment process

Assessing and mitigating the risk of ML/TF is not a static exercise. The risks you identify may change or evolve over time as new products, services, affiliations, or developments and technologies enter your business or its environment. You should be regularly reassessing the ML/TF-related risks to your business and documenting that assessment to keep it up to date. For example, if you add a new product, service or technology to your business, or open a new location, you should evaluate and document the associated risks of this change to your business.²³⁴

FINTRAC's guidance on the risk-based approach to combatting money laundering and terrorist financing describes its risk-based approach (RBA) as a six-step cycle for AML/ATF and explains what FINTRAC's expectations are for your RBA. In summary, these are that you:

- identify your inherent risks
- set your risk tolerance
- create risk-reduction measures and key controls
- evaluate your residual risks
- implement your RBA
- review your RBA

The risk assessment process is a consultative process throughout the organization which allows for a thorough understanding of the business structure along with all areas of risk.

As an example, the first step in the risk assessment process is identifying where within your organization triggering activities are being conducted and classifying those activities into the correct category of inherent risk.

²³⁴ FINTRAC, *Risk assessment guidance*, August 4, 2021

For instance, the business consulting team at an accounting firm may purchase and sell businesses on behalf of their clients. Determining what activities are being conducted can involve interviews with partners or service line leads to obtain an adequate understanding of the business to determine if triggering activities are being conducted or could be conducted in the future. A questionnaire can be used if the organization is large with offices across the country. Once it has been determined where the activities are being conducted and which specific ones they are, a risk rating can be completed on each specific triggering activity.

FINTRAC's guidance provides assistance with the risk rating process and allows for objective classification using established criteria. For instance, services that allow for client anonymity are recommended to be rated as high-risk services. This criterion can be applied to triggering activities because it is not a requirement to identify a client unless they have provided funds of \$3,000 and above, conducted a large cash or virtual currency transaction, or conducted/attempted a suspicious transaction or you know/believe that they have or control terrorist property. Therefore, any triggering activity that does not involve a trigger for the verification of identity may be classified as high risk. This example is meant as a guide and, in practice, many other factors can be considered in the risk rating process of all products and services.

Regardless of the risk rating, it is important to provide rationale for the rating and to ensure that the reasons provided are reasonable. The level of risk associated to each triggering activity will determine if any additional enhanced measures need to be taken. For activities deemed to be low or medium risk, it is not a requirement to have enhanced measures, but if the risk of the activity is high, enhanced measures are mandatory. In the example above, if the transaction is conducted without requiring identification and it is deemed high risk, additional enhanced measures should be documented and conducted.

6.3.3.1 Risk assessment

The compliance program is to include a documented risk assessment of the risk of money laundering and the terrorist financing offence. The risk assessment involves assessing and documenting the risks, taking into consideration the following five risk categories.

6.3.3.1.1 *Clients and business relationships*

This factor should fully explain all clients that you are dealing with and it should consider the nature of the relationship with the clients. It is about understanding your clients and the types of activities and transactions that they normally conduct. The nature of the relationships should consider things such as the length of the relationship and how the client was acquired or introduced. Certain client industries are considered a higher risk of money laundering and/or terrorist financing, such as cash-intensive businesses, and these elements should be considered within the risk of each client. For instance, the risk level of a client with a convoluted legal structure based in a known client offshore secrecy jurisdiction would, all else being equal, be a higher risk client than an individual client engaged in a personal tax return service. It is recommended that a list of low, medium and high-risk business types be created that can be used objectively for all future clients. The same process is recommended for occupation types

6.3.3.1.2 *Products and delivery channels*

Elements to consider within this factor include itemizing all products and services that are offered and assessing the risk of money laundering and/or terrorist financing associated with each specific product and service. For instance, the risk associated with a short tax engagement may be lower than the risk of an extensive investment advisory engagement spanning several years. The delivery channels through which products and services are offered also need to be analyzed within this risk factor. Specifically, you need to consider how the products and services are actually delivered to your clients. For instance, are all clients serviced through face-to-face meetings or are there any offerings available through non-face-to-face methods? The risk of having non-face-to-face delivery methods would, all else being equal, be higher than face-to-face as the ability to disguise identification becomes easier with the increase in distance between the service/product supplier and the client. It is recommended that a list of all products and services be created along with their associated risk. Any products or services that are determined to be a high risk of money laundering and/or terrorist financing would require your organization to document enhanced measures when those products or services are offered.

6.3.3.1.3 *Geographic location of the activities*

It is important to consider the geographic locations in which your organization operates in addition to the geographic location of your clients. Specific to area of operations, the level of detail may be as high-level as a breakdown by province or as granular as an office-by-office risk assessment. The crime level

and prevalence of specific criminal activities are elements to consider when completing the assessment of geographic risk of your operations. As well, the same framework will guide your organization in assessing the geographic location of your clients. However, the geographic location of the client may be included in their specific risk assessment. It is recommended that a risk scoring be done on all office locations to rank them according to risk

6.3.3.1.4 *New developments and impact of new technologies*

As noted previously, the AML/ATF legislation requires that if you plan to carry out a new development or introduce a new technology that may have an impact on your clients, business relationships, products, services or delivery channels or the geographic location of their activities, you must assess and document the risk before doing so. If the risk is high, you are required to take special measures.²³⁵

6.3.3.1.5 *Any other relevant factor*

Within this “catch-all” remaining factor, things to consider include all elements outside of the first four factors. For instance, what is the level of turnover within your organization? Is there a restriction placed on staff members before they successfully complete AML/ATF training? The risk of money laundering and/or terrorist financing will increase for these elements if the turnover is high and there are no restrictions to staff responsibilities prior to completing training. It is recommended that for staff working in areas more prone to money laundering and/or terrorist financing risks, restrictions or oversight be placed upon their day-to-day activities until such a time as their training has been successfully completed.

6.3.4 Risk mitigation

The purpose of the risk assessment is to apply a risk-based approach where resources are appropriately allocated to address high risk areas. The risk assessment should also include risk mitigation measures. This means that where you have identified areas of high risk, you have to take special measures, also known as enhanced measures (see Section 6.3.6), to mitigate the risks to a level to which you are comfortable taking into account your risk tolerance.

The AML/ATF legislation prescribes special measures that are to be applied for identified areas of high risk. These measures can be specific to the prescribed factor or can be applied directly to the clients if they are deemed high risk.

²³⁵ PCMLTFR subsection 156(2) and PCMLTFA subsection 9.6(2)

6.3.5 Ongoing monitoring of triggering activity business relationships

Ongoing monitoring is a process that you must develop and use to review all the information you have obtained about the clients with whom you have a business relationship, in order to:

- detect any suspicious transactions that you are required to report to FINTRAC
- keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date
- reassess the level of risk associated with your client's transactions and activities
- determine whether transactions or activities are consistent with the client information you obtained and your risk assessment of the client²³⁶

Pursuant to the AML/ATF legislation, accountants and accounting firms must recognize the establishment of a “business relationship” with any client for which two or more triggering activities are performed and client identification is required within any rolling five-year period.²³⁷ That is, a business relationship is established for every client for which two or more transactions occur involving the creation of a receipt of funds record and a large cash, large virtual currency, suspicious transaction, or terrorist property report is filed within any rolling five-year period. You should determine that a business relationship has been established as soon as possible after the second transaction or activity where you had to verify the client's identity. As a best practice, this should be done within 30 calendar days after the second transaction or activity.

If a business relationship has been created by two STRs you may decide to treat the business relationship as posing a high risk, and undertake more frequent ongoing monitoring, as well as take any other appropriate enhanced measures.

The establishment of a business relationship gives rise to the immediate obligation to keep a record that sets out the “purpose and intended nature of the business relationship.” This record should include information that would help you anticipate the types of transactions and activities your client may conduct. It should best describe your business dealings with a client.

²³⁶ PCMLTFR subsection 123.1 and FINTRAC, *Ongoing monitoring requirements*, August 4, 2021.
²³⁷ PCMLTFR paragraph 4.1(b)

If you already keep this information in another record, then you do not need to create a new record.

All of the measures and the definition of purpose and intended nature of the business relationship are with reference only to triggering activities. Non-triggering activities (such as the performance of an audit engagement) are to be excluded from the analysis.

Measures undertaken to conduct ongoing monitoring, as well as findings and outcomes, must be documented. Ideally, all ongoing monitoring for any given client is conducted on the same cycle to achieve efficiencies.

6.3.5.1 *Defining the purpose and intended nature of a business relationship*

In FINTRAC's guidance²³⁸ a non-exhaustive list of three potential "purpose and intended nature of business relationship" descriptions is suggested such as:

- transferring funds or securities
- paying or receiving funds on behalf of a client, or
- purchasing or selling assets or entities

The "purpose and intended nature of business relationship" must be recorded in a business relationship record created at the inception of the business relationship. FINTRAC guidance suggests that the information recorded is meant to assist in understanding the client's activities over time, and that a determination could be achieved through a combination of information on hand and inquiries of the client. In professional accounting scenarios, the engagement letter typically documents the client's objectives (purpose of the business relationship) and services to be offered (nature of the business relationship). It is critical that policies and procedures reflect the adoption of that information source for the determination if that is the approach taken by the accountant or accounting firm.

6.3.5.2 *Ongoing monitoring: Detecting suspicious transactions and assessing the consistency of transactions with client knowledge and risk*

An ongoing monitoring exercise to detect suspicious transactions for a client with which an accountant or accounting firm has established a business relationship for triggering activities would generally involve a historical review of triggering activities conducted in the period under the review. The review frequency and scope would depend on the assessment of the client's risk and should be documented. Triggering activity transactions would generally

238 FINTRAC, *Business relationship requirements*, August 4, 2021

be compared against expectations and in view of suspicious transaction indicators, for a perspective that might not have arisen for consideration of each triggering activity transaction in isolation.

6.3.5.3 *Ongoing monitoring: Keeping client identification information up to date*

Keeping client identification up to date for clients with which the accountant or accounting firm has established a business relationship must occur with a frequency commensurate with the client's money laundering risk. Updating client information does not involve re-identifying the client – re-identification should generally occur only when the veracity of identification is in question, or when a client is not recognized in the course of a transaction attempt. Client information updates, rather, involve re-confirming and updating information regarding client identification which might change over time, such as legal name, address and occupation. The measures taken and outcomes must be documented contemporaneously.

6.3.5.4 *Ongoing monitoring: Reassessing client risk levels*

As explained in Section 6.3 Assess and document the risk of ML/TF and Section 6.3.4 Risk mitigation, client risk levels are determined with reference to their characteristics, products and services, delivery channels, relevant geographic locations, introduction of new technology and other relevant factors. Through ongoing monitoring with a frequency determined by the pre-existing risk level, client risk is re-evaluated against risk factors established by the accountant or accounting firm. Based upon a review of the client's activities and transactions and the updated client information, it may result in a higher or lower risk assessment for the client. For instance, if the client has reduced the amount of activity and their transactions have become less frequent, all else being equal, their risk level may be reduced to low from medium. The opposite is also true where, based on a change in client information and activity, the level of risk can be raised from low to medium or high. The rationale for changes to the risk level should reflect the risk assessment methodology established when the risk assessment documentation was created.

FINTRAC has indicated in its guidance that it expects that your policies and procedures will include the frequency at which you will conduct ongoing monitoring of your clients, based on your risk assessment for a client or group of clients.

6.3.5.5 *When does ongoing monitoring end?*

Once your business relationship ends, you are no longer required to conduct ongoing monitoring.

6.3.6 Enhanced measures²³⁹

Where you have identified a client to be high risk, the AML/ATF legislation prescribes special measures (enhanced measures) that are to be applied.

Enhanced measures are the additional controls and processes that you have put in place to manage and reduce the risks associated with your high-risk clients and business areas. As part of your compliance program, you must develop and apply written policies and procedures for the enhanced measures that you will take for any ML or TF risks you identify as high.²⁴⁰

Your policies and procedures for enhanced measures must include:²⁴¹

- the additional steps, based on assessment of the risk, that you will take to verify the identity of a person or entity
- any other additional steps that you will take to mitigate the risks, including, but not limited to, the additional steps to:
 - ensure client identification information and beneficial ownership information is updated at a frequency that is appropriate to the level of risk
 - conduct ongoing monitoring of business relationships at a frequency that is appropriate to the level of risk

Enhanced measures to mitigate risk can include:

- obtaining additional information on a client (for example, information from public databases and the internet)
- obtaining information on the client's source of funds or source of wealth²⁴²
- obtaining information on the reasons for attempted or conducted transactions, or
- any other measures you deem appropriate

This means that you must take enhanced measures and conduct ongoing monitoring of a client you have identified as high risk. These are extra measures in addition to what is required, as appropriate for the level of client risk.²⁴³

²³⁹ PCMLTFR section 157

²⁴⁰ PCMLTFA subsection 9.6(3)

²⁴¹ PCMLTFR section 157

²⁴² FINTRAC, *Guidance Glossary*, May 4, 2021 and Section 3.5.1 of this guide for definitions of source of funds and source of wealth

²⁴³ PCMLTFR paragraph 157(b)(ii)

Enhanced measures — general

You may consider the following methods to conduct enhanced ongoing monitoring for high-risk clients:²⁴⁴

- reviewing transactions based on an approved schedule that involves management sign-off
- developing reports and reviewing these reports of high-risk transactions more frequently
- flagging certain activities or those that deviate from your expectations and raise concerns, as necessary
- setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review, or
- reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships

Enhanced measures — client specific

The following enhanced measures can be utilized for high-risk clients:

- requiring that more than one piece of an acceptable photo identification document be accepted when required to verify the client's identification²⁴⁵
- requiring a second piece of identification when required to verify the client's identification
- confirming the address of the client by requesting affirming documentation such as a utility bill or cable bill with a matching name
- confirming the occupation by requesting affirming documentation such as an employment letter or recent pay stub to confirm the current occupation
- obtaining additional information on a client (e.g., volume of assets, information available through public databases, Internet, etc.)
- obtaining information on the source of funds or source of wealth of a client
- when dealing with an entity:
 - requiring that a status of corporation be provided instead of articles of incorporation to ensure the corporation is still active
 - verifying the identification of all directors or authorized signers of the entity

²⁴⁴ FINTRAC, *Ongoing monitoring requirements*, August 4, 2021

²⁴⁵ There are documented cases of persons having more than one driver's license with differing information on each.

- confirming the entity’s operations by conducting a physical drive-by of the premises or using a browser (e.g., Google Street View) to confirm the address is existent and the physical location is consistent with the entity’s nature, purpose and operations
- asking for beneficial ownership information on all clients that are entities
- verifying insider/beneficial ownership information of publicly traded companies on the System for Electronic Disclosure by Insiders (SEDI)²⁴⁶
- reviewing the client’s activity on a pre-determined frequency, such as every six months or annually, for any suspicious transactions
- internet searches for any negative news matches on individual clients or directors/signing officers from an entity client
- checking names against a reputable names list such as World-Check for potential Politically Exposed Foreign Persons (PEFP), Politically Exposed Domestic Persons (PEDP), their family members and close associates, upon the creation of an engagement

Enhanced measures — products, services, delivery channels, geographic location

The following enhanced measures can be utilized for high-risk factors:

- for geographical areas ranked high-risk, requiring secondary approval of all transactions
- prohibiting certain transactions if the client is domiciled in a high-risk geographical area
- requesting source of funds/source of wealth documentation for clients in high-risk areas
- requesting additional identification when offering products or services deemed high-risk
- obtaining information on the reasons for attempted or conducted transactions
- increasing the frequency of your monitoring of higher-risk transactions, products, services and channels
- gathering additional documentation, data or information, or take additional steps to verify the documents you have obtained
- establishing transaction limits
- increasing internal controls for high-risk business relationships

²⁴⁶ System for Electronic Disclosure by Insiders (SEDI)

- obtaining the approval of senior management for products and services that are new for clients
- any other measures you deem appropriate

Ultimately the enhanced measures are those that go above and beyond what is required for regular transactions to satisfy standard legislative requirements. It should be noted that a combination of measures may be used depending on the specific situation and when warranted.

6.3.6.1 When does the requirement for enhanced monitoring end?

You are no longer required to conduct enhanced ongoing monitoring when your business relationship ends or when, based on your risk assessment, you no longer consider a client to pose a high risk. When you no longer consider a client high-risk, you are still required to conduct ongoing monitoring of the client at the frequency determined by the client's new risk rating.²⁴⁷

6.3.7 FINTRAC examination

FINTRAC examination of risk assessment

FINTRAC has indicated that during an examination, it may examine:²⁴⁸

- your risk assessment, your controls and mitigating measures including your policies and procedures, to assess the overall effectiveness of your risk assessment
- your business relationships to evaluate whether they have been properly assessed based on the products, services, delivery channels, geographical risk and other characteristics or patterns of activities
- your high-risk client files to ensure that the prescribed special measures have been followed and applied
- sample records to assess whether monitoring and reporting are done in accordance with legislation, regulations and your policies and procedures

FINTRAC has also indicated that it may:²⁴⁹

- verify that you have assessed and documented the risks to your business related to money laundering and terrorist activity financing and that you have identified measures to mitigate these risks and applied special measures for any high risks

²⁴⁷ FINTRAC, *Ongoing monitoring requirements*, August 4, 2021

²⁴⁸ FINTRAC, *Risk assessment guidance*, August 4, 2021

²⁴⁹ FINTRAC, *Assessment manual*, Section 3.1.3, March 21, 2022

- verify that you have assessed and documented risk using a risk-based approach before you implement a new development or introduce a new technology that may affect your clients, business relationships, products, services or delivery channels, or the geographic location of your activities, and may also review the process you follow before introducing new developments or new technologies
- verify that you have assessed risks adequately by looking at the areas you have identified as posing a high risk and the assessment's written rationale. FINTRAC may review a sample of client records and records of transactions in order to determine whether your risk assessment is reasonable and consistent with your business's risk profile, and policies and procedures
- verify whether you document and apply special measures to elements you have determined pose a high risk. Special measures include taking enhanced measures to identify clients and to mitigate risks such as keeping client identification information up-to-date and conducting ongoing monitoring for the purpose of detecting suspicious transactions, as well as any other enhanced measures you identify
- verify that the controls you have in place are consistent with your identified risk levels (rankings) and adequately mitigate your business risks
- verify that your compliance program is in line with and informed by the results of your risk assessment. For example, FINTRAC will confirm that your policies and procedures, ongoing training documentation and two-year review documentation adequately address the areas you have assessed as posing a higher risk and that they provide adequate guidance to your employees or agents
- verify how you use publicly available information to inform your compliance program
- interview the employees and agents responsible for your risk assessment to assess their knowledge of the requirements associated with conducting a risk assessment

FINTRAC has also indicated in its guidance that it expects that your policies and procedures will include the frequency at which you will conduct ongoing monitoring of your clients, based on your risk assessment for a client or group of clients.

FINTRAC's focus will be on verifying that you have considered and rated the risk of all aspects of your business, that you have provided rationales for your decisions, and that you have applied special measures to areas identified as posing a high risk.

6.4 Ongoing training program

If as an accountant or accounting firm you have employees, agents or mandataries or other persons who are authorized to act on your behalf, you must develop and maintain a written, ongoing compliance training program for those employees, agents or mandataries or other persons.²⁵⁰

Your training program should explain what your employees, agents or mandataries, or other persons authorized to act on your behalf, need to know and understand, including:

- your requirements under the AML/ATF legislation
- background information on ML/TF, such as the definition of ML/TF and methods of ML/TF
- how your profession could be vulnerable to ML/TF activities (provide indicators and examples). This should help with the identification of suspicious transactions and may provide you some assurance that your services are not being abused for ML/TF purposes.
- the compliance policies and procedures you have developed to help meet your requirements under the AML/ATF legislation for preventing and detecting ML/TF, including your reporting, record keeping and know your client requirements
- your roles and responsibilities in detecting and deterring ML/TF activities, and when dealing with potentially suspicious activities or transactions. These can range from day-to-day tasks to high-risk situations.

The persons to be trained would include anyone who interacts with clients, anyone who sees client transaction activities, anyone who handles virtual currencies, cash or funds in any way and anyone who is responsible for implementing or overseeing the compliance program.

The ongoing compliance training program is required to be in writing. Although the AML/ATF legislation does not state what specifically is to be included in the written training program, there are certain expectations of

²⁵⁰ PCMLTFR subsection 156(1)(d) and FINTRAC, *Compliance program requirements*, August 4, 2021.

what the ongoing training program should cover. FINTRAC's guidance and its assessment manual provide direction on what should be included in the ongoing training program.

6.4.1 FINTRAC examination

FINTRAC has indicated that during an examination, it may examine your training program.

FINTRAC uses the following methods to verify your compliance with the requirement to develop and maintain a written ongoing compliance training program for employees or agents.

FINTRAC examination of your training program²⁵¹

FINTRAC:

- looks at who receives training, what topics are covered, when and how often training takes place, how you have implemented your training program and how training is delivered
- verifies that your training program is adequate, takes into account the size, type, nature and complexity of your business, and is put into practice

FINTRAC may:

- review your policies and procedures to confirm that they provide enough guidance to your employees, agents and those acting on your behalf to develop, implement and maintain an ongoing training program
- review your training plan to confirm that it considers and documents the steps you take to develop, maintain and deliver your training program
- review your training material to confirm that the training content is suitable, for example, verify that it is tailored to your business and adequate for your employees, agents and their respective responsibilities
- interview your employees and agents to confirm that they understand the requirements as they relate to their positions, understand and follow the policies and procedures, understand how your business could be vulnerable to ML/TF activities and have received adequate ongoing training

251 FINTRAC, *Assessment manual*, Section 3.1.4, March 21, 2022

FINTRAC's focus is on whether your training program helps your employees and agents understand the requirements, your policies and procedures, and indicators and trends of money laundering and terrorist activity financing. FINTRAC also pays close attention to the training you provide regarding the detection of suspicious transactions.

6.5 Instituting and documenting a training plan and delivering compliance training²⁵²

The AML/ATF legislation also requires that you institute and document a plan for your ongoing compliance training program and for delivering the training.²⁵³ Your training plan should cover how you will implement your ongoing compliance training program and its delivery. This includes documenting the steps you will take to ensure your employees, agents or mandataries, or other persons authorized to act on your behalf receive an appropriate level of training relevant to their duties and position, on an ongoing basis. Your training plan should include information about the following: training recipients, training topics and materials, training methods for delivery and training frequency.

Your training plan should explain who will receive training. Training recipients should include those who:

- have contact with clients, such as front-line staff or agents
- are involved in client transaction activities
- handle cash, funds or virtual currency for you, in any way
- are responsible for implementing or overseeing the compliance program (such as the compliance officer, senior management, information technology staff or internal auditors)

6.5.1 Training topics and material

Your training plan should outline the topics that will be covered in your training program. It should also include the sources of the training materials that will cover these topics.

²⁵² FINTRAC, *Compliance program requirements*, August 4, 2021
²⁵³ PCMLTFR subsection 156(1)(e)

The actual content of the training program should focus on the areas of greatest importance and would ideally be role specific. In an accounting firm, the most important concept to teach all staff members is the definition of a triggering activity and how to recognize one when it occurs. This key piece of information is a prerequisite to all requirements that come because of the triggering activity being conducted and should be understood by all staff at your organization. The various indicators of suspicious transactions should be taught to all staff as well. Staff members are the first line of defense regarding flagging suspicious transactions to the compliance team and being aware of what types of transactions to flag will go a long way in the goal of having an effective compliance program. Finally, the training material should also include a step-by-step process for all staff upon receiving funds for an engagement that includes triggering activities. These three areas are a must for all staff to understand and should be expanded on depending on the specific role that the staff member has at your organization.

You should also consider including how you will address new hire training and any restrictions on their responsibilities prior to completion of training and how to address individuals that were not present for training.

Helpful content resources could include: FATF's Methods and Trends Publications as well as FINTRAC's various publications on typologies, operational alerts, etc.

6.5.2 Training methods for delivery

Your training plan should describe the training method(s) that you will use to deliver your ongoing compliance training program. Training methods could include self-directed learning (where recipients read materials on their own, register for online courses or use e-learning materials), information sessions, face-to-face meetings, classroom, conferences, and on-the-job training where instruction is provided. Instructors can be in-house personnel or an external service provider, but they should have knowledge of the AML/ATF legislation. If you decide to use in-house personnel, you may need to hire or allocate staff to provide training. If you decide to use an external service provider, you may need to determine whether their services and training content are suitable for your business. You can use one or more training methods. The method(s) that you choose may depend on the size of your business and the number of people that need to be trained.

6.5.3 Training frequency

Your training plan should describe the frequency of your ongoing compliance training program. Training can be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur (for example, before a new employee deals with clients, after a procedure is changed), or by using a combination of both.

Your ongoing compliance training program and plan should be tailored to your business's size, structure and complexity, and its degree of exposure to ML/TF risk. For example, if you are a large accounting firm, you may decide to provide different types of training to your employees, agents or mandataries, or other persons authorized to act on your behalf based on their specific roles and duties (for example, general or specialized training). This should be explained in your training plan.

Your training program should also include a record of the training that has been delivered (for example, the date the training took place, a list of the attendees who received the training, the topics that were covered). Training records will help you keep track of the training and assist you in scheduling the next training dates. They will also demonstrate that you are carrying out your training program on an ongoing basis.

Note: If you are an accountant with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program nor are you required to have a training plan in place for yourself

6.5.4 Sample training plan

A training plan shows that you have ongoing training in place. It also provides a summary of your ongoing training program that can be used to manage internal resources when it comes to training. The training plan should align with your ongoing training program and indicate who is to receive training and when training is to roll out. It is important to ensure that the material provided to staff is in context to their role within the organization. The following is a sample training plan. It is recommended that the date of each training effort be documented.

Table 6 – Sample training plan and schedule

Type of staff	Identifying triggering activities	Know your client, business relationships, and ongoing monitoring, beneficial ownership and record keeping	Money laundering methods and detection	Reporting transactions	FINTRAC examination process
Leadership	Annual		Annual		
Designated compliance officer	Annual	Annual	Ongoing	Annual	Annual
Professional staff	Annual	Bi-Annual	Annual	Bi-Annual	
Administrative	Annual	Annual	Annual	Annual	

6.6 Review and test the effectiveness of your compliance program

Accountants and accounting firms are required to institute and document a plan for a review of the compliance program every two years to test its effectiveness.²⁵⁴ You must start your review no later than 24 months from the start of your previous review. You must also ensure that you have completed your previous review before you start the next review. The purpose of an effectiveness review is to determine whether your compliance program has gaps or weaknesses that may prevent you as an accountant or an accounting firm from effectively detecting and preventing ML/TF. Your effectiveness review will help you determine if:

- your business practices reflect what is written in your compliance program documentation and if you are meeting your requirements under the AML/ATF legislation

²⁵⁴ PCMLTFR paragraph 156(1)(f), and subsections 156(3) and (4)

- your risk assessment is effective at identifying and mitigating the ML/TF risks related to your clients, products, services, delivery channels, new developments or technology, and geographic locations where you do business

The review must be carried out and the results documented by an internal or external auditor, or by yourself if you do not have an auditor.²⁵⁵ Your review should be conducted by someone who has an adequate working knowledge of your requirements under the AML/ATF legislation. Also, as a best practice, to ensure that your review is impartial, it should not be conducted by someone who is directly involved in your compliance program activities.

Important note: If you are an entity, you must report, in writing, the following to a senior officer no later than 30 days after the completion of the effectiveness review:²⁵⁶

- the findings of the review (for example, deficiencies, recommendations, action plans)
- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself
- the status of the implementation of the updates made to your policies and procedures

You should also document the following in your two-year effectiveness review:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review
- the results of the tests that were performed
- the conclusions, including deficiencies, recommendations and action plans, if any

6.6.1 Requirement for instituting and documenting of a plan for the two-year effectiveness review

You must also institute and document a plan for the two-year effectiveness review of your compliance program.²⁵⁷ This plan should describe the scope of the review and must include all the elements of your compliance program.

²⁵⁵ PCMLTFR subsection 156(3)

²⁵⁶ PCMLTFR subsection 156(4)

²⁵⁷ PCMLTFR 156(1)(f)

The breadth and depth of review for each element may vary depending on factors such as the complexity of your business, transaction volumes, findings from previous reviews, and current ML/TF risks. Your plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

6.6.2 Evaluation methods²⁵⁸

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation. The following are examples of what can be included in your review:

- interviews with those handling transactions to evaluate their knowledge of your policies and procedures and related record keeping, client identification and reporting requirements
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC
- a review of LCTRs, LVCTRs, STRs and TPRs to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines
- a review of a sample of your client records to see whether the risk assessment was applied in accordance with your risk assessment process
- a review of a sample of your client records to see whether the frequency of your ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken
- a review of a sample of your records to confirm that proper record keeping procedures are being followed
- a review of your risk assessment to confirm that it reflects your current operations
- a review of your policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect your current business practices

6.6.2.1 *Additional elements you may consider testing during your review*

Examples of other areas you may consider testing in your effectiveness review could include:

258 FINTRAC, *Compliance program requirements*, August 4, 2021

- **policies and procedures:**
 - verifying that the procedures are actually being adhered to by staff on a consistent basis throughout the organization
 - collecting a sample of large cash and large virtual currency transactions followed by a review of the reporting of these transactions
- **risk assessment:**
 - checking for the presence of all prescribed factors within the risk assessment documentation
 - checking for the presence of inherently low, medium and high-risk factors and analyzing whether the risk rankings are current and accurate to the organization
 - checking for the presence of policy statements related to the risk-based approach specific to high-risk areas that require mitigation measures
 - testing high risk areas through a review of client information and transactions to verify whether the risk mitigation measures have been followed
 - reviewing reported STRs and any transactions flagged as unusual to verify the process specific to high-risk clients:
 - » a sample of your clients followed by a review to see if the risk assessment was applied correctly
 - » a sample of your clients followed by a review to see if the frequency of your ongoing monitoring is adequate
 - » a sample of high-risk clients followed by a review to ensure that enhanced mitigation measures were taken
- **training program:**
 - comparing the training material against the specific recipient role within the organization to test the applicability
 - testing whether all applicable staff are receiving training and whether any gaps exist through a comparison of current and past employees against a training tracking sheet
 - reviewing any testing materials in place to ensure that appropriate questioning is being used
 - checking staff quiz/test scores to test the process of adequate retention of material

6.6.3 Sample scope

The effectiveness review should include the scope of the review that takes into account the required component of the compliance program. Below is a sample scope that can be used to ensure that all components are being covered in the effectiveness review:

Table 7 – Sample scope

Required components	Scope	Items to test
Policies and procedures	Document evaluation	AML/ATF policies and procedures
	Operational evaluation	FINTRAC reports <ul style="list-style-type: none"> • receipt of funds records • client identification and verification records • business relationships records • beneficial ownership records • PEP, HIO, their family and close associate records • capture and retention of other applicable records
Risk assessment	Document evaluation	Risk assessment documents <ul style="list-style-type: none"> • procedures/methodology of risk assessment • procedures on enhanced measures for high-risk clients • documented risk assessment of organization
	Operational evaluation	High-risk clients <ul style="list-style-type: none"> • application of enhanced measures • ongoing monitoring processes
Training program	Document evaluation	Ongoing training program Training materials
	Operational evaluation	Training log Interviews with staff to test knowledge of AML/ATF

Included in Chapter 33 Appendix S – Self-review checklist is a checklist an accountant or accounting firm can consider using to evaluate their progress towards an effective compliance program.

6.6.4 FINTRAC examination²⁵⁹

In an examination, FINTRAC will verify that you conduct, every two years at a minimum, a review of your policies and procedures, risk assessment, and training program for the purpose of testing their effectiveness. FINTRAC will verify that your two-year effectiveness review is adequate, tailored to your business by taking into account the type, nature, size and complexity of your business, and consistent with your risk assessment.

FINTRAC examination of your review and testing of policies and procedures

In conducting this examination, FINTRAC may:²⁶⁰

- review your documented plan to verify that it considers all the elements of your compliance program for the purpose of testing its effectiveness
- review your policies and procedures to determine whether they give enough guidance to your employees or agents to conduct a two-year effectiveness review
- look at the scope of the review (what the review covered) and methodology (how the review was conducted):
 - interview the person who conducted the review to learn about its scope and methodology, and to ensure that they understand all the requirements that apply to your business
 - when looking at the scope, for example, FINTRAC assesses whether your policies and procedures, risk assessment and ongoing compliance training program have been reviewed and cover the current legal requirements and your current operations. They also confirm that the review covers and tests all the requirements applicable to your sector
 - when looking at the methodology, for example, FINTRAC verifies whether the review was carried out by an internal or external auditor, or by you if you do not have an auditor; whether it was conducted within the required timelines; and whether the testing methods and methodology used were adequate and reasonable

259 FINTRAC, *Assessment manual*, March 21, 2022

260 FINTRAC, *Assessment manual*, Section 3.1.5, March 21, 2022

- verify that a written report was provided to a senior officer within 30 days of the review, and that the report included the findings of the review, updates made to the policies and procedures within the reporting period of the review, and the status of the implementation of these updates
- verify that the findings of the review are being actioned

FINTRAC's focus will be to verify that your review:

- assesses whether you have a well-documented compliance program and that your program is adequately put into practice
- adequately identifies areas where you did not meet your requirements, whether you updated your policies and procedures, and the status of these updates

CHAPTER 7

Receiving funds of less than \$3,000? What to do.

The AML/ATF legislation defines funds as (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash. It does not include virtual currency.²⁶¹

When receiving funds of less than \$3,000 you are not required to keep records, submit reports or verify the identify of clients, unless there is a need to file a suspicious transaction or a Terrorist Property Report. If so, refer to Chapters 9 and 11 respectively of this guide.

7.1 Do you consider the activities to be high risk?

Despite the relatively low amount of funds being received (less than \$3,000), the activities that your client may be involved in and the transactions may be determined to be high risk. If in your risk assessment you have assessed the client's transaction to be high risk, then you must take special measures (enhanced measures) to mitigate the risk of ML/TF. These special measures are described in Section 6.3.6.

²⁶¹ PCMLTFR subsection 1(2)

7.2 Do you have a business relationship with the client?²⁶²

The requirements related to the determination of business relationship and ongoing monitoring of that business relationship is described in greater detail in Section 4.2.2.

A business relationship is a relationship established between you and a client to conduct financial transactions or provide services related to financial transactions. A business relationship²⁶³ established for an accountant or accounting firm the second time within a five-year period that the accountant or accounting firm is required to verify the identity of the client when engaged in triggering activities.

You do not enter into a business relationship that would otherwise have been formed after the first or second time you are required to verify identity, if you are not required to verify the identity of a client under the regulations because of a related exception. This is because your obligation to verify identity for a particular transaction, activity or client does not apply in that circumstance. For example, if your requirement to verify identity does not apply because your client is a public body, a very large corporation (e.g., a corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet),²⁶⁴ or a subsidiary of either of those, whose financial statements are consolidated, then a business relationship would not be formed.

However, a business relationship would be formed in instances where you have the obligation to verify identity, but the AML/ATF legislation allows you to not do so for a particular reason. This is because the underlying obligation to verify a client's identity still exists, even if you relied upon the applicable reasoning for not verifying identity. This could occur as the result of a suspicious transaction or attempted transaction, or as the result of not having to re-verify the identity of a client.²⁶⁵

- **Suspicious transaction reporting**

When you are required to submit an STR to FINTRAC, you are required to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct the transaction. Despite whether your reasonable measures are unsuccessful, or if you believe

²⁶² FINTRAC, *Business relationship requirements*, August 4, 2021

²⁶³ PCMLTFR paragraph 4.1(b) and FINTRAC, *Business relationship requirements*, August 4, 2021

²⁶⁴ PCMLTFR paragraphs 154(2)(a) to (p)

²⁶⁵ FINTRAC, *Business relationship requirements*, August 4, 2021

taking reasonable measures would inform the person or entity that you are submitting a STR, this transaction must factor into your business relationship requirements, if it is the second time you are required to verify the identity of a client.

- **Re-verifying identity:**

Your business relationship requirements must still factor in a transaction or activity for which you have the requirement to verify identity but choose not to because the AML/ATF legislation allows it. The AML/ATF legislation allows you to choose not to re-verify the identity of a client if:

- you previously did so using the methods specified in the AML/ATF legislation in place at the time
- you have kept the associated records
- you have no doubts about the information used²⁶⁶

If you submitted a STR or a TPR to FINTRAC on two occasions for this client (in this section, we are referring to a transaction when dealing with the receipt of less than \$3,000. You should keep in mind that there are no dollar thresholds for submitting a STR or TPR), you will have had the obligation to verify the identity of the client twice, hence a business relationship would have been created. The establishment of a business relationship gives rise to the immediate obligation to keep a business relationship record (Section 26.1.2 Sample - Record of Business Relationship Information) that sets out the “purpose and intended nature of the business relationship,”²⁶⁷ then the ongoing obligations²⁶⁸ to periodically monitor the business relationship and keep an ongoing business relationship record²⁶⁹ recording the measures taken when you conduct ongoing monitoring of the business relationship with that person or entity and of the information obtained from that ongoing monitoring on a risk-sensitive basis, for the purpose of:²⁷⁰

1. detecting any reportable suspicious transactions or attempted suspicious transactions
2. keeping client identification information up to date
3. reassessing the level of risk associated with the client’s transactions and activities
4. determining whether transactions or activities are consistent with the information obtained about the client, including the risk assessment of the client

266 PCMLTFR section 155

267 PCMLTFR section 145

268 PCMLTFR subsection 123.1

269 PCMLTFR section 146(1)

270 PCMLTFR section 123.1

All of the measures and the definition of purpose and intended nature of the business relationship are with reference only to Triggering Activities. Non-Triggering Activities (such as the performance of an audit engagement) are to be excluded from the analysis.

Measures undertaken to conduct ongoing monitoring, as well as findings and outcomes, must be documented. Ideally, all ongoing monitoring for any given client is conducted on the same cycle to achieve efficiencies.

7.3 If you have a business relationship with the client, is the client a PEP, HIO, a family member or close associate (of foreign PEP only, in certain circumstances)?

If it is determined that you are in a business relationship with the client, you must take reasonable measures²⁷¹ to make a business relationship related PEP, HIO, family member²⁷² or close associate (of foreign PEP only, in certain circumstances) determination when you:

- enter into a business relationship
- conduct periodic monitoring of your business relationships
- detect a fact about your existing business relationships that indicates a PEP or HIO connection

²⁷¹ FINTRAC, *Guidance Glossary*, May 4, 2021

²⁷² FINTRAC, *Guidance Glossary*, May 4, 2021

CHAPTER 8

Receiving funds of \$3,000 or more? What to do.

The AML/ATF legislation defines funds as (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash. The definition of funds does not include virtual currency.²⁷³

If funds of \$3,000 or more are received by an accountant or accounting firm in a single transaction in connection with a triggering activity, four task obligations are triggered:

1. Keep a receipt of funds record.
2. Verify the identity of the client and keep a record of verification of identity of the client from whom the funds are received.
3. Keep a business relationship and ongoing business relationship monitoring record (if applicable).
4. Keep a record beneficial ownership to confirm the accuracy of beneficial ownership information (if applicable).

Those funds might be received in respect of fees, or for any other reason connected with the triggering activity. The AML/ATF legislation does not specify that the funds must be received from the client for which the triggering activity is being performed. However, if the funds received are \$10,000 or more in cash or virtual currency in a single transaction (in accordance with the 24-hour rule), you have additional requirements. These requirements are explained in Chapter 10. You may also have requirements to report a suspicious transaction (see Chapter 9) and terrorist property (see Chapter 11).

²⁷³ PCMLTFR subsection 1(2)

8.1 Keep a receipt of funds record

When an accountant or accounting firm engages in a triggering activity, the AML/ATF legislation requires that a receipt of funds record be completed for every amount of \$3,000 or more of funds (in cash or in another form) in the course of a single transaction. However, the definition of funds does not include virtual currency.²⁷⁴

All fields in the receipt of funds record are mandatory. A sample receipt of funds record and instructions are provided in Chapter 22 Appendix H.

The receipt of funds record must include:²⁷⁵

- the date of the receipt
- if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation
- if the amount is received from or on behalf of an entity, the entity's name and address and the nature of its principal business
- the amount of the funds received and of any part of the funds that is received in cash
- the method by which the amount is received
- the type and amount of each fiat currency involved in the receipt
- if applicable, the exchange rates used and their source
- the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder
- the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth
- every reference number that is connected to the transaction and has a function equivalent to that of an account number
- the purpose of the transaction

If the receipt of funds record relates to a client that is a corporation,²⁷⁶ you must also keep a copy of the part of the official corporate records that contains any provision relating to the power to bind the corporation regarding the transaction. Official records can include a certificate of incumbency, the

²⁷⁴ PCMLTFR subsection 1(2)

²⁷⁵ Ibid

²⁷⁶ PCMLTFR paragraph 52(b)

articles of incorporation or the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.²⁷⁷

If there were changes subsequent to the articles or bylaws that related to the power to bind the corporation regarding the transaction, and these changes were applicable at the time the transaction was conducted, then the board resolution stating the change would be included in this type of record.

The receipt of funds record must be retained for five years after the date of its creation.²⁷⁸ Receipt of funds records should not be filed with FINTRAC; however, their details might be subsequently referenced as necessary in a suspicious transaction report (see Chapter 9), a large cash transaction report (see Chapter 10) or in a Terrorist Property Report (see Chapter 11).

8.1.1 General exceptions

Record keeping obligations are exempted under certain conditions. The general exception in the AML/ATF legislation allows an accountant or an accounting firm that is required to keep a record to NOT include information in that record that is readily obtainable from other records that they are required to keep under the AML/ATF legislation.²⁷⁹ This means that if you keep the required information and can produce it during a FINTRAC examination you do not need to create a new record to meet your obligations.

The AML/ATF legislation provides that the requirement to verify the identity of clients using the prescribed verification methods in certain situations no longer applies if, after taking reasonable measures, the accountant or accounting firm is unable to obtain the information. Reasonable measures²⁸⁰ means that you must take steps to collect certain information, even if taking those steps did not result in the desired information being obtained. For example, this can include doing one or more of the following: asking the client, conducting open-source searches, or consulting commercially available information. Those reasonable measures must be recorded.

8.1.2 Specific exceptions

You are NOT required to keep a receipt of funds record if:

²⁷⁷ See Section 20.4 of this guide for FINTRAC Policy Interpretation PI-6409 dated 2016-03-30

²⁷⁸ PCMLTFR paragraph 148(1)(c)

²⁷⁹ PCMLTFR section 153

²⁸⁰ FINTRAC, *Guidance glossary*, May 4, 2021

- you must keep a large cash transaction record for the same transaction
- the funds are received from a financial entity,²⁸¹ a public body or from a person who is acting on behalf of a client that is a financial entity or public body

A receipt of funds record is also specifically exempted under the AML/ATF legislation²⁸² when accountants or accounting firms, where applicable, are engaged in triggering activities in respect of:

- a. the sale of an exempt policy as defined in subsection 306(1) of the Income Tax Regulations
- b. the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component
- c. the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation
- d. the sale of a registered annuity policy or a registered retirement income fund
- e. the sale of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy
- f. a transaction that is part of a reverse mortgage or structured settlement
- g. the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation
- h. the opening of an account in the name of an affiliate of a financial entity, if the affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Act
- i. the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account
- j. the opening of an account established in accordance with the escrow requirements of a Canadian securities regulator or Canadian stock exchange or provincial legislation

281 PCMLTFR subsection 1(2) **financial entity** means (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act; (b) a financial services cooperative; (c) a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy; (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and (iii) advance payments to which the policy holder is entitled that are made to them by the insurer; (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and (e) a department, or an entity that is an agent of Her Majesty in right of Canada or an agent or mandatary of Her Majesty in right of a province, when it carries out an activity referred to in section 76.

282 PCMLTFR subsection 154(2)

- k. the opening of an account if the account holder or settlor is a pension fund that is regulated under federal or provincial legislation
- l. the opening of an account in the name of, or in respect of which instructions are authorized to be given by, a financial entity, a securities dealer, a life insurance company or an investment fund that is regulated under provincial securities legislation
- m. a public body
- n. a corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act and that operates in a country that is a member of the FATF
- o. a subsidiary of a public body referred to in paragraph (m) or a corporation or trust referred to in paragraph (n) whose financial statements are consolidated with the financial statements of that public body, corporation or trust; or
- p. the opening of an account solely in the course of providing accounting services to a securities dealer

8.2 Verify the identity of the client and keep a record

When you receive \$3,000 or more in funds when engaged in a triggering activity, you must verify the identity of the person you are dealing with or, if the client is an entity, verify the identity of the entity.

In instances where funds are received unexpectedly and without the client present, and where the client had not been previously identified, the accountant or accounting firm should identify the client prior to processing or returning the funds (both to meet regulatory obligations and to establish ownership over the property).

8.2.1 Verifying the identity of persons

You must identify a person²⁸³ (an individual/natural person) providing you **funds** in the amount of \$3,000 or more in a single transaction, **at the time the transaction takes place**,²⁸⁴ whether or not it is in cash or in another form (but not virtual currency if it is less than \$10,000), although as a best practice, it should occur as soon as practical after being engaged to conduct a triggering activity.

²⁸³ PCMLTFR subsection 105(1)
²⁸⁴ PCMLTFR paragraph 105(7)(a)

The AML/ATF legislation allows the use of one of four different methods of verifying a person's identity for accountants and accounting firms.²⁸⁵

The four methods available to accountants and accounting firms are:²⁸⁶

1. government-issued photo identification method
2. credit file method
3. dual-process method
4. reliance method

The AML/ATF legislation also allows you to verify the identity of a person when relying on an agent or mandatary, as long as one of the four identification methods described above are used and certain conditions are met.

These requirements and identification methods are further detailed in Chapter 23, Appendix I – Verifying the identity of a person.

Exceptions to the verification of identity for a person are listed in Section 23.10.

8.2.1.1 Keeping a record of verification of the identity of a person

When you are required to verify a person's identity you must keep a record of information specific to the four prescribed methods used.²⁸⁷ Chapter 23 provides details of the information to be recorded and samples of the records to keep when dealing with a person.

- Sample record when referring to a **government-issued photo identification** method is available in Section 23.3.3 of this guide.
- Sample record when referring to information in a client's **credit file** is available in Section 23.4.2 of this guide.
- Sample record when referring to information using the **dual method** is available in Section 23.5.4 of this guide.

You may **rely on an agent or mandatary** to carry out the verification on your behalf in accordance with one of the three following methods: government-issued photo identification method, the credit file method or the dual-process method. You also have record keeping obligations specific to each method. The information required to be recorded is listed in Section 23.7 of this guide.

²⁸⁵ For greater clarity, a fifth method is only applicable to reporting entities covered under the PCMLTFA under paragraphs 5(a) to 5(g) which do not include accountants and accounting firms.

²⁸⁶ PCMLTFR paragraphs 105(1)(a) to (d) and FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021.

²⁸⁷ PCMLTFR section 108 and FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021.

8.2.2 Verifying the identity of an entity²⁸⁸

Where an entity is the client for triggering activities, the accountant or accounting firm must verify the identity and confirm the existence of the entity. While an entity can be a **corporation** or **an entity other than a corporation** such as a trust, a partnership, a fund or an unincorporated association or organization, corporations are subject to different requirements than other entities.

In summary, two methods are available to accountants and accounting firms to verify the identity of an entity:

1. confirmation of existence method
2. reliance method

8.2.2.1 Confirmation of existence method for a corporation

Using this method to verify a corporation's identity you may refer to:

- its certificate of incorporation
- a record that it is required to file annually under applicable provincial securities legislation, or
- the most recent version of any other record that confirms its existence as a corporation and contains its name and address and the names of its directors such as a certificate of active corporate status, the corporation's published annual report signed by an audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government²⁸⁹

The record you refer to must be authentic, valid and current.²⁹⁰ You may obtain a corporation's name and address and the names of its directors from a publicly accessible database, such as a provincial or federal database like the Corporations Canada database,²⁹¹ or a corporation search and registration service through subscription.

The methods verifying the identity and existence of **corporations** are described in detail in this guide in Chapter 24, Appendix J - Verifying the identity of an entity and other requirements and specifically, in Section 24.1.1.

8.2.2.2 Confirmation of existence method for an entity other than a corporation

Using this method to verify the identity of an **entity other than a corporation** you may refer to:²⁹²

288 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

289 Ibid

290 PCMLTFR subsection 109(2)

291 Corporations Canada, [Search for a Federal Corporation \(database\)](#)

292 PCMLTFR subsection 112(1)

- a partnership agreement
- articles of association, or
- the most recent version of any other record that confirms its existence and contains its name and address

The confirmation method verifying the identity and existence of an entity other than a corporation is described in detail in this guide in Chapter 24 Appendix J - Verifying the identity of an entity and in Section 24.1.2.

Verifying the existence of a corporation²⁹³ or an entity other than a corporation²⁹⁴ must occur within 30 days after the day on which the transaction is conducted.

Note: Your compliance program’s policies and procedures must describe the processes you follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how you will ensure that the information is authentic, valid and current.

8.2.2.3 *Reliance method*

You may verify the identity of a **corporation** or **other entity** by relying on the measures that were previously taken by **another reporting entity (RE)** (a person or entity that is referred to in section 5 of the PCMLTFA).²⁹⁵

To rely on the measures previously taken by **another RE** to verify the identity of a corporation or an entity other than a corporation, you must:²⁹⁶

- as soon as feasible, obtain from the **other RE** the information that was used to confirm the identity of the corporation or an entity other than a corporation, as the case may be, and be satisfied that:
 - the information is valid and current²⁹⁷
 - **for a corporation**, its identity was verified by the **other RE** by referring to a record as described in the confirmation of existence method above, **or** if the measures to verify the corporation’s identity were performed prior to June 1, 2021, that the **other RE** confirmed the corporation’s existence and ascertained its name, address, and the names of its directors in accordance with the methods in the PCMLTFR as they read at that time²⁹⁸

293 PCMLTFR paragraph 109(4)(i)

294 PCMLTFR paragraph 112(3)(i)

295 PCMLTFR paragraphs 110(1)(a) and 113(1)(a)

296 PCMLTFR paragraphs 110(3) and 113(3)

297 See *FINTRAC Glossary* or this guide at Section 3.5.1 for definitions of “valid” and “current”

298 PCMLTFR paragraph 110(3)(a)

- **for an entity other than a corporation**, its identity was verified by the **other RE** by referring to a record as described in the confirmation of existence method above, or if the measures to verify the entity's identity were performed prior to June 1, 2021, the **other RE** confirmed the entity's existence in accordance with the methods in the PCMLTFR as they read at that time²⁹⁹
- have a written agreement or arrangement in place with the **other RE** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the identity of the **corporation** or other **entity**, as the case may be³⁰⁰

Note: Your compliance program's policies and procedures must describe the processes you follow when using the reliance method to verify the identity of corporations and other entities and how you will ensure that the information is valid and current.

8.2.2.4 Record keeping requirements

If you refer to a paper record or an electronic version of a record, you must keep the record or a copy of it.

If the electronic version of the record that you refer to is contained in a database that is accessible to the public, you must keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.³⁰¹

8.2.2.5 Exceptions

You do not have to verify:

- the identity of a corporation or an entity other than a corporation for subsequent transactions or activities, as required, if:
 - you have already verified the identity by using the **confirmation of existence method** and referred to a paper or electronic record, or
 - prior to June 1, 2021:³⁰²
 - » **in the case of an entity**, you confirmed the entity's existence in accordance with the PCMLTFR, and you complied with the related record keeping provisions, as they read at the time, or

²⁹⁹ PCMLTFR paragraph 113(3)(a)

³⁰⁰ PCMLTFR paragraphs 110(3)(b) and 113(3)(b)

³⁰¹ PCMLTFR subsections 109(5) and 112(4)

³⁰² PCMLTFR subsections 155(2) and 155(3)

- » **in the case of a corporation**, you confirmed the corporation's existence and ascertained its name and address and the names of its directors in accordance with PCMLTFR, and you complied with the related record keeping provisions, as they read at the time

However, you must not have doubts about the information that was previously used to verify the identity of the corporation or other entity. If you have doubts, you must verify identity again using the methods explained in this guide in accordance with the PCMLTFR and FINTRAC's guidance.³⁰³

Other exceptions:

You do not need to verify the:

- identity of a person or entity in connection with the receipt of funds of \$3,000 or more, if the client is: a public body, a very large corporation or trust, or a subsidiary of those types of entities, if the financial statements of the subsidiary are consolidated with those of the public body, very large corporation or trust³⁰⁴

You do not need to:

- take reasonable measures to identify the individual who conducts or attempts to conduct a suspicious transaction, only if:
 - you have already identified the individual as required and have no doubts about the identification information
 - you believe that identifying the individual would inform them that you are submitting a suspicious transaction report
- when a corporation is a securities dealer, confirm the names of a corporation's directors when you confirm its existence, if the corporation is a securities dealer³⁰⁵

You are not subject to the AML/ATF legislation as an accountant or accounting firm if the activities you undertake are in the course of an audit, review or compilation engagements, or carried out within the meaning of the CPA Canada Handbook.³⁰⁶

Exceptions to the verification of the identity and existence of an entity are also described in Section 24.4.

³⁰³ PCMLTFR subsections 155(1), 155(2), 155(3) and FINTRAC *Methods to verify the identity of persons and entities*, footnote 34, November 19, 2021

³⁰⁴ PCMLTFR paragraphs 154(2)(m), (n) and (o)

³⁰⁵ PCMLTFR subsection 109(3)

³⁰⁶ PCMLTFR subsection 47(2)

8.3 Keep a business relationship and ongoing business relationship monitoring record (if applicable)

Because you have received funds of \$3,000 or more, you are required to verify the identity of your client. As an accountant or accounting firm you enter into a business relationship with a client the **second time** that you are required to verify the identity of the client within a five-year period.³⁰⁷

When this occurs you must:

- collect and record the nature and purpose of the business relationship with the client³⁰⁸

The AML/ATF legislation also requires that when you enter into a business relationship with a client you must periodically conduct, based on a risk assessment,³⁰⁹ ongoing monitoring³¹⁰ of that business relationship for the purpose of:

1. detecting a suspicious or attempted suspicious transaction or a terrorist activity financing transaction or attempted terrorist activity financing transaction that must be reported
2. keeping client identification information, beneficial ownership³¹¹ and business relationship³¹² information referred to up to date
3. reassessing the level of risk associated with the client's transactions and activities
4. determining whether transactions or activities are consistent with the information obtained about their client, including the risk assessment of the client

In the course of ongoing monitoring of the business relationship you must:

- take reasonable measures to confirm the accuracy of the beneficial ownership information of an entity³¹³
- keep a record of the measures taken of the business relationship with that person or entity
- keep a record of the information obtained from that ongoing monitoring and enhanced ongoing monitoring of high-risk clients³¹⁴

³⁰⁷ PCMLTFR paragraph 4.1(b) and FINTRAC, *Business relationship requirements*

³⁰⁸ PCMLTFR subsection 145

³⁰⁹ PCMLTFA subsection 9.6(2). The risk assessment must be undertaken in accordance with PCMLTFR paragraph 156(1)(c)

³¹⁰ PCMLTFR subsection 123.1

³¹¹ PCMLTFR section 138

³¹² PCMLTFR section 145

³¹³ PCMLTFR subsection 138(2)

³¹⁴ PCMLTFR subsection 146(1)

You must keep records of the measures you take and of the information obtained from the ongoing monitoring of your clients with whom you have a business relationship.³¹⁵ This includes:

- your processes in place to perform ongoing monitoring
- your processes in place to perform the enhanced ongoing monitoring of high-risk clients
- your processes for recording the information obtained as a result of your ongoing monitoring
- your processes for recording the information obtained as a result of your enhanced ongoing monitoring of high-risk clients
- the information obtained as a result of your ongoing monitoring and enhanced ongoing monitoring of high-risk clients

You must outline the measures you use to conduct the ongoing monitoring of your business relationships in your policies and procedures, which can form part of your ongoing monitoring records. However, the information you obtain as a result of your ongoing monitoring is likely to be specific to a particular business relationship and not captured in your policies and procedures, so it should be documented separately. You can document and update the information you obtain through your ongoing monitoring activities across several records. For example, updates to the client identification, beneficial ownership or business relationship information you have, could be recorded in any file you maintain on a client.³¹⁶

As a record to collect the required information, you may use the form in Section 26.1.2 – Sample – Record of business relationship information.

8.4 Keep a record of beneficial ownership and reasonable measures (if applicable)

At the time you verify the identity of an entity, you must also obtain information about its beneficial ownership.³¹⁷ In all cases (except for not-for-profit organizations), you must collect information establishing the ownership, control and structure of the entity.³¹⁸ If you established a business relationship with that client, you must also confirm the accuracy of the beneficial ownership information in the course of ongoing monitoring. The information you must collect is as follows and summarized in Table 8 below:

³¹⁵ PCMLTFR subsection 146(1)

³¹⁶ FINTRAC, *Ongoing monitoring requirements*, August 4, 2021

³¹⁷ PCMLTFR subsection 138(1)

³¹⁸ PCMLTFR paragraph 138(1)(d)

In the case of a corporation, you must obtain the names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation, and information establishing the ownership, control and structure of the entity.³¹⁹

In the case of a widely held or publicly traded trust, you must obtain the names of all trustees of the trust and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust³²⁰ and information establishing the ownership, control and structure of the entity.

In the case of a trust, you must obtain the names and addresses of all trustees and all known beneficiaries and settlors of the trust and information establishing the ownership, control and structure of the entity.³²¹

In the case of an entity other than a corporation or trust, you must obtain the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity³²² and information establishing the ownership, control and structure of the entity.

In the case of a not-for-profit organization, you must keep a record that sets out whether that entity is (a) a charity registered with the CRA under the Income Tax Act; or (b) an organization, other than one referred to in paragraph (a), that solicits charitable donations from the public.³²³

You may use the form in Section 25.7 of this guide, Sample - Record of beneficial ownership, as an example to record the above information.

319 PCMLTFR paragraphs 138(1)(a) and (d)

320 PCMLTFR paragraphs 138(1)(a.1) and (d)

321 PCMLTFR paragraphs 138(1)(b) and (d)

322 PCMLTFR paragraphs 138(1)(c) and (d)

323 PCMLTFR subsection 138(5)

Table 8

Entity type	Information to collect	
Corporation	Names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation	Information establishing the ownership, control and structure of the entity
Widely held or publicly traded trust	Names of all trustees of the trust and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust	
Trust	Names and addresses of all trustees and all known beneficiaries and settlors of the trust	
Entity other than a corporation or trust	The names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity	
Not-for-profit organization	Determine if it is a charity registered with the CRA under the Income Tax Act, or an organization, other than a charity registered with the CRA under the Income Tax Act, that solicits charitable donations from the public.	

You must take reasonable measures to confirm the accuracy of the information when it is first obtained and in the course of ongoing monitoring of business relationships. You must keep a record that sets out the information and the measures taken to confirm the accuracy of the information.

If you are unable to obtain the information, to keep it up to date in the course of ongoing monitoring of business relationships or to confirm its accuracy, you must take:

- reasonable measures to verify the identity of the entity's chief executive officer or the person who performs that function
- special measures referred to in section 157 of the PCMLTFR which are:
 - a. taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity
 - b. taking any other enhanced measure to mitigate the risks, including:
 - i. ensuring, at a frequency appropriate to the level of risk, that client identification information and beneficial information is up to date
 - ii. conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships to:

- a. detect suspicious transactions
- b. keep client identification information, beneficial ownership and business relationship information up to date
- c. reassess the level of risk associated with your client's transactions and activities
- d. determine whether transactions or activities are consistent with the information obtained about your client, including the risk assessment of the client

CHAPTER 9

Report a suspicious transaction or attempted transaction

9.1 What is a suspicious transaction report (STR)?

According to the AML/ATF legislation, accountants and accounting firms are required to report to FINTRAC, using the prescribed form, every financial transaction that occurs or is attempted in the course of triggering activities and in respect of which there are **reasonable grounds to suspect (RGS)**³²⁴ that the transaction is related to the commission or the attempted commission of (a) a money laundering offence; or (b) terrorist activity financing offence.³²⁵ This must be done as **soon as practicable** after you have taken **measures** (see Section 9.2 of this guide for a description of these measures) that enable you to establish RGS.³²⁶

This requires accountants and accounting firms to submit a suspicious transaction report (STR) to FINTRAC when they reach the RGS threshold. The STR must be completed whether the suspicious transaction is conducted or attempted. RGS means that there is a possibility that an ML/TF offence has occurred. In these circumstances you must report to FINTRAC, using the prescribed forms, electronically or on paper, the attempted and completed suspicious transactions which relate to triggering activities.

³²⁴ See Section 9.2 of this guide for an explanation of the meaning of RGS and FINTRAC, *What is a suspicious transaction report?*, August 12, 2021

³²⁵ PCMLTFA section 7

³²⁶ FINTRAC, *Reporting suspicious transactions to FINTRAC*, August 12, 2021

As soon as practicable should be interpreted to mean that you have completed the measures that have allowed you to determine that you reached the RGS threshold and as such the development and submission of that STR must be treated as a priority report. FINTRAC expects that you are not giving unreasonable priority to other transaction monitoring tasks and may question delayed reports. The greater the delay, the greater the need for a suitable explanation. FINTRAC's guidance is that STRs can be complex yet you must treat them as a priority and ensure they are timely; you must also complete the measures that enabled you to conclude that you have reasonable grounds to suspect the commission of an ML/TF offence before you submit the report to FINTRAC.

The explanation of your assessment should be included in the narrative portion, Part G, of the STR. Many factors will support your assessment and conclusion that an ML/TF offence has possibly occurred; they should be included in your report to FINTRAC.

There is no monetary threshold associated with the reporting of a suspicious transaction under the AML/ATF legislation. However, there may be situations where a single transaction will trigger the requirement to submit more than one report to FINTRAC. For example, if a completed transaction reported in an STR involved the receipt of cash from a client of \$10,000 or more, you would also be required to report this transaction to FINTRAC in a large cash transaction report.

You must report electronically to FINTRAC unless you do not have the technical capability to do so. A sample form is included at Chapter 21 Appendix G — Suspicious Transaction Report form.³²⁷ FINTRAC also provides guidance on the reporting of STRs.³²⁸

FINTRAC assesses and analyzes the data from all reports, including STRs, and other data sources to create a picture that serves to uncover financial relationships and networks that will:

- assist law enforcement (i.e., designated recipients of its financial intelligence disclosures) in investigating or prosecuting offences related to ML/TF, as well as threats to the security of Canada³²⁹
- detect trends and patterns related to ML/TF risks

³²⁷ Reporting directly to FINTRAC via secure internet or using a paper format is explained on [FINTRAC's website](#).

³²⁸ FINTRAC, [What is a suspicious transaction report?](#), August 12, 2021

³²⁹ PCMLTFA subsections 55(3) and 55.1(1)

- uncover vulnerabilities of Canada's financial system
- enhance public awareness of ML/TF matters

One of the most valuable and unique report types submitted to FINTRAC is the STR. In addition to the prescribed information, STRs allow for an expansion on the descriptive details surrounding a transaction that is derived from your assessment of what you are seeing through your business interactions and activities. Additional information, such as nicknames, secondary names, beneficial ownership information, IP addresses, additional account numbers, email addresses, virtual currency transaction addresses and their details, details of purchases or e-transfers, locations, relationships and background information are all additional details that FINTRAC uses in its analysis and production of financial intelligence disclosures.

Because of the importance of FINTRAC's financial intelligence to the overall safety and security of Canadians and Canada's financial system, FINTRAC reviews and assesses every STR it receives. When warranted, such as in the case of STRs related to threats to the security of Canada, FINTRAC expedites its analysis in order to disclose financial intelligence to law enforcement and other intelligence partners within 24 hours.

Failing to submit an STR, or not submitting an STR in a timely manner, may directly affect FINTRAC's ability to carry out its mandate. Therefore, FINTRAC expects that when you have completed your measures and determined that you have reached RGS that a transaction is related to the commission of an ML/TF offence, you will prioritize the submission of that STR.

If you are in receipt of a production order, by law enforcement, you must perform an assessment of the facts, context and ML/TF indicators to determine whether you have RGS that a particular transaction is related to the commission of ML/TF.

9.1.1 TPR vs STR

TPRs differ from other reports that are submitted to FINTRAC because a transaction or attempted transaction does not have to occur for you to submit a TPR. Instead, it is the mere existence of property (such as a bank account) owned or controlled by or on behalf of a terrorist group or listed person that prompts your obligation to submit a TPR.³³⁰

³³⁰ FINTRAC, *Reporting terrorist property to FINTRAC*, August 4, 2021

TPRs contribute to Canada's AML and ATF regime as they provide information about property held by a terrorist group or a listed person that may not be found in other financial transaction reports. In addition, through FINTRAC's tactical analysis, TPRs can provide invaluable insight and assist in the detection of individuals and entities that may be involved in terrorist activity financing networks.

Money laundering. The offence of **money laundering** in Canada broadly involves a person who deals with property or proceeds of any property **they know, they believe or are being reckless** as to whether all or a part of that property was derived directly or indirectly as a result of a designated offence committed in Canada or elsewhere, with the intent to conceal or convert³³¹ that property or those proceeds.³³² Designated offences include all manner of offences that can generate proceeds and could result in jail sentences of two years or more (even murder for hire). Particularly, they include offences related to drugs, fraud, theft, robbery, tax evasion, copyright, as well as break and enter. According to FINTRAC, the person reporting the transaction need not have knowledge or suspicion of the specific offence that gave rise to the proceeds, only RGS that reported transactions are related to money laundering or terrorist financing.

Terrorist financing. The offence of **terrorist financing** generally involves providing or collecting property intending or knowing that it will be used in whole or in part to carry out a terrorist activity. Terrorist activity includes such things as acts committed for a political, religious, ideological purpose with the intention of intimidating the public with regard to economic or physical security, or compelling any person, government or international organization to do or to refrain from doing any act, and that intentionally causes or endangers health, property, services, facilities or systems.³³³ Research has found that the methods employed for money laundering and terrorist financing are similar.

Terrorist property. Once you **know** that any property in your possession or control is owned or controlled by or on behalf of a terrorist or a terrorist group, or after any transaction is made or proposed for such a property, a **TPR**³³⁴ must be sent to FINTRAC immediately. If you know that a transaction is related to property owned or controlled by or on behalf of a terrorist

331 Convert means to change or transform and does not require an element of concealment (R. v. Daoust, [2004] 1 SCR 217, 2004 SCC 6).

332 Criminal Code of Canada subsection 462.31(1).

333 Criminal Code of Canada Section 2

334 FINTRAC, *Reporting terrorist property to FINTRAC*, August 4, 2021

or a terrorist group, **you should not complete it**. This is because such property must be frozen under the Criminal Code. The government maintains a list of entities they have reasonable grounds to believe have knowingly carried out, attempted to carry out, participated in or facilitated terrorist activity; or knowingly acting on behalf of such an entity.³³⁵

If a transaction was attempted or completed, and it involved property that you **know** is owned or controlled by or on behalf of a terrorist group, **you should also submit an STR** to FINTRAC. This is because you have reached the threshold of **reasonable grounds to suspect** that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence.

Listed person. Once you **believe** that any property in your possession or control is owned or controlled by or on behalf of a **listed person**, or after any transaction is made or proposed for such a property, a **TPR** must be sent to FINTRAC immediately. (For more details refer to Chapter 11). If you know that a transaction is related to property owned or controlled by or on behalf of a listed person, **you should not complete it**. This is because such property must be frozen under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*.

If a transaction was attempted or completed, that you **believe** is owned or controlled by or on behalf of a listed person (for which you must submit a TPR), **you should also submit an STR** to FINTRAC. This is because you have reached the threshold of **RGS** that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence.

Unsure but suspect. However, if you are **not sure that you are dealing with a terrorist or terrorist group**, or a listed person but suspect that you might be, then an **STR** is required if a transaction was completed or attempted.

9.2 Establish reasonable grounds for suspicion

RGS is the required threshold to submit an STR to FINTRAC and is a step above simple suspicion, meaning that there is a **possibility** that an ML/TF offence has occurred. FINTRAC's Guidance on STRs³³⁶ explains that reaching RGS means that you consider the **facts, context** and **ML/TF indicators**

³³⁵ Public Safety Canada, *Currently listed entities*, June 21, 2019
³³⁶ FINTRAC, *What is a suspicious transaction report?*, August 12, 2021

related to a financial transaction and, after having reviewed this information, you conclude that there are RGS that this particular financial transaction is related to ML/TF. You must be able to demonstrate and articulate your suspicion of ML/TF in such a way that another individual reviewing the same material with similar knowledge, experience or training would likely reach the same conclusion.

You do not have to verify the **facts, context** or **ML/TF indicators** that led to your suspicion, nor do you have to prove that an ML/TF offence has occurred in order to reach RGS. Your suspicion must be reasonable and therefore, not biased, or prejudiced.

Understanding the differences between the thresholds between **simple suspicion, reasonable grounds to suspect** (RGS) and **reasonable grounds to believe** can help clarify what RGS means for accountants and accounting firms and how it can be operationalized within your compliance program.³³⁷

Simple suspicion is a lower threshold than RGS and is synonymous with a “gut feeling” or “hunch.” In other words, simple suspicion means that you have a feeling that something is unusual or suspicious, but do not have any facts, context or ML/TF indicators to support that feeling or to reasonably conclude that an ML/TF offence has occurred. Simple suspicion could prompt you to assess related transactions to see if there is any additional information that would support or confirm your suspicion.

Reasonable grounds to believe is a higher threshold than RGS and is **beyond** what is required to submit an STR. Reasonable grounds to believe means that there are verified facts that support the probability³³⁸ that an ML/TF offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe, not just suspect**, that ML/TF has occurred. For example, **law enforcement** must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a production order.³³⁹

If you are in receipt of a production order, by law enforcement, you must perform an assessment of the facts, context and ML/TF indicators to determine whether you have RGS that a particular transaction is related to

³³⁷ FINTRAC, *What is a suspicious transaction report?, Diagram 1*, August 12, 2021

³³⁸ FINTRAC, *Guidance Glossary*: Probability means the **likelihood** in regard to completing a suspicious transaction report (STR) that a financial transaction **is related** to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence.

³³⁹ FINTRAC, *Guidance Glossary*: Production order means a judicial order that compels a person or entity to disclose records to peace officers or public officers.

the commission of ML/TF. If you identify a transaction whereby you reach reasonable grounds to believe that an ML/TF offence has occurred, you must begin an assessment of the related transactions immediately as you have surpassed the RGS threshold. If assessed by FINTRAC and there are reasonable grounds to believe that a transaction is related to the commission of an ML/TF offence, and you have not begun an assessment of the facts, context or ML/TF indicators, you may be cited for a missed STR. In situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, you are encouraged, as a best practice, to expedite the submission of your STRs. FINTRAC recommends that this be included in your policies and procedures.

One way of identifying potentially suspicious transactions is to be vigilant about indicators of money laundering (see Chapters 30 and 31) at the time of the transaction. Another is through the conduct of ongoing monitoring and enhanced measures applied to clients and their activities (discussed in Section 4.2.2.2).

In order to submit an STR to FINTRAC, you will need to ensure that you have completed the **measures** that enable you to reach your reasonable grounds to suspect the commission of ML/TF. These measures include:

- screening for and identifying suspicious transactions
- assessing the facts and context surrounding the suspicious transaction
- linking ML/TF indicators to your assessment of the facts and context
- explaining your grounds for suspicion in an STR, where you articulate how the facts, context and ML/TF indicators allowed you to reach your grounds for suspicion

What is a fact? A fact, for the purpose of completing an STR, is defined as an event, action, occurrence or element that exists or is known to have happened or existed – it cannot be an opinion. For example, facts about a transaction could include the date, time, location, amount or type. Facts known to you could also include account details, particular business lines, the client’s financial history or information about the individual or entity (for example, that the individual has been convicted of a designated offence or is the subject of a production order, or that an entity is being investigated for fraud or any other indictable offence).

What is context? Context, for the purpose of completing an STR, is defined as information that clarifies the circumstances or explains a situation or transaction. This type of information is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario. You may observe or understand the context of a transaction through:

- a general awareness of the events occurring in an individual or entity's business environment or community
- your knowledge of the typical financial activities found within your business
- regular know your client (KYC) activities (for example, confirming identification details of the individual, their occupation or business, how they generate their wealth, their typical or expected transactional behaviours, etc.)
- the information obtained through the application of your risk-based approach
- illustrative client details (for example, the background, behaviour and actions of your client)

A transaction may not appear suspicious in and of itself. However, a review of additional contextual elements surrounding the transaction may create suspicion. Conversely, the context of a particular transaction, which may have seemed unusual or suspicious from the onset, could lead you to reassess your client's current and past transactions and conclude that they are reasonable in that circumstance.

What is an ML/TF indicator? ML/TF indicators are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically stem from one or more facts, behaviours, patterns or other factors that identify irregularities related to a client's transactions. These transactions often present inconsistencies with what is expected or considered normal based on the facts and context you know about your client's transactional activities.

FINTRAC published ML/TF indicators for each reporting entity sector, including for accountants and accounting firms. These were developed through a three-year review of ML/TF cases, a review of high-quality STRs, and literature published by international organizations such as the FATF and the Egmont Group, and in consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation; they are meant to provide all reporting entity sectors with a general understanding

of what is or could be considered unusual or suspicious. FINTRAC also publishes operational alerts and briefs that offer additional information on the identification of ML/TF related methods, techniques and vulnerabilities.

On its own, an indicator may not initially appear suspicious. However, it could lead you to question the legitimacy of a transaction, which may prompt you to assess the transaction to determine whether there are further facts, contextual elements or additional ML/TF indicators that would increase your suspicion to the point where submitting an STR to FINTRAC would be required.

Criminal organizations often try to avoid the detection of ML/TF by using multiple concealment methods. Indicators of ML/TF can bring to light suspicious transactional activity, but it is your holistic assessment of facts, context and ML/TF indicators that will enable you to determine whether you have reached RGS that a transaction is related to the commission of an ML/TF offence. Indicators are also helpful to articulate your rationale for RGS in an STR. The explanation of how you reached your grounds for suspicion is extremely important for FINTRAC's development and disclosure of financial intelligence.

Putting it all together. Your suspicion of ML/TF will likely materialize from your assessment of multiple elements (transactions, facts, context, and any other related information that may or may not be an indicator of ML/TF). When these elements are viewed together, they create a picture that will either support or negate your suspicion of ML/TF.

The explanation of your assessment should be included in the narrative portion, Part G, of the STR. Many factors will support your assessment and conclusion that an ML/TF offence has possibly occurred; they should be included in your report to FINTRAC.

The occurrence of a suspicious transaction also gives rise to an obligation to take reasonable measures to verify the identity of a person that attempts or conducts the suspicious transaction unless that person had been previously identified according to the AML/ATF legislation, or if conducting the identification would make the person aware that a report was being filed (known as “tipping off”).

9.3 Verification of client identity and no tipping off

See Chapter 23 for all requirements relating to the verification of identity of a person and an entity.

It is an offence to disclose that an STR has been filed, or to disclose the content of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun.³⁴⁰ However, it is common practice in other industries for reporting entities to request clarifying information about transactions for the purpose of enhanced measures, without reference to STR obligations.

9.4 Complete the STR

Completed and attempted suspicious transactions can be reported to FINTRAC either electronically, if the accountant/accounting firm has the technical capability to do so, or, otherwise, in paper format. A copy of the paper form is attached in Chapter 21, Appendix G — Suspicious transaction report form along with field-by-field guidance on completing the report. A copy must be retained for five years following the transaction(s) and filed with FINTRAC as soon as practicable³⁴¹ after establishing reasonable grounds to suspect. All fields marked with an asterisk are mandatory fields. All other fields are “reasonable measures”³⁴² fields, which mean that they must be completed if the information is available to the accountant or accounting firm.

FINTRAC has identified the suspicious transaction narrative portion of the report (known as section G) as being the most critical to their intelligence objectives. In addition to detailing reasons for suspicion, FINTRAC desires these information elements in the narrative: the names of individuals and entities involved in transactions; directorships and signing authorities for business entities; account numbers and other key identifiers (e.g., date of birth, government-issued ID, addresses, telephone numbers); the flow of funds; historical transaction activity; and associated entities and individuals and relationships between them (e.g., family members, business associates).

³⁴⁰PCMLTFA section 8

³⁴¹ PCMLTFSTRR subsection 9(2): The person or entity shall send the report to the Centre as soon as practicable after they have taken measures that enable them to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.

³⁴² PCMLTFSTRR subsection 11(1) and (2)

9.5 Record keeping

There are two records to keep when submitting an STR:

- The first is maintaining a copy of the STR. The AML/ATF legislation requires that you keep a copy of all reports sent to FINTRAC.³⁴³ It serves as a Suspicious Transaction Record, since the mandatory fields of the report cover all the requirements of the record.
- The second record to keep is the verification of client identity record. See Chapter 23 for all requirements relating to the verification of identity of a person and an entity. If possible, client identity verification should precede the completion of the record and report to obtain all necessary details (so long as those steps can be completed, and the report filed “as soon as practicable”) and the client is not “tipped off” about the submission of the STR.

Specifically, when it comes to obtaining the identity of a person or entity, the reporting obligations under the AML/ATF Legislation³⁴⁴ require that you take reasonable measures when completing an STR. It states that you must “... take reasonable measures to verify, in accordance with section 105, 109 or 112 [of the PCMLTFR], the identity of a person or entity that conducts or attempts to conduct a transaction with them that is required to be reported to the Centre under section 7 of the Act.”

9.6 Exceptions

As an accountant or an accounting firm, the suspicious transaction reporting requirement does not apply to the receipt of professional fees.³⁴⁵

You do not have to take reasonable measures to identify the individual who conducts or attempts to conduct a suspicious transaction only if:

- you have already identified the individual as required and have no doubts about the identification information, or
- you believe that taking the reasonable measures to identify the individual would inform them (tipping off) that you are submitting a STR³⁴⁶

³⁴³ PCMLTFR section 144

³⁴⁴ PCMLTFR subsection 85(1) and Section 7 of the PCMLTFA

³⁴⁵ FINTRAC, *Reporting suspicious transactions to FINTRAC*, August 12, 2021

³⁴⁶ PCMLTFR subsections 85(1) and (2)

9.7 FINTRAC examination³⁴⁷

FINTRAC uses a variety of assessment methods to ensure that you are detecting suspicious transactions and submitting complete reports in a timely manner. During an assessment, FINTRAC expects that you will be able to:

- confirm that you have an ongoing monitoring process, and have measures described in your policies and procedures and risk assessment (that is, enhanced measures and special measures for high-risk activities and clients) that are operationalized to enable the timely detection, assessment and, when required, reporting of suspicious transactions
- demonstrate your process for identifying relevant transactions
- explain how your process for detecting and assessing suspicious transactions is effective, reasonable and consistent with your risk assessment, and applied across all your business lines
- demonstrate that you have a risk-based process and that it is incorporated in your decision-making processes for the submission of STRs

In assessing what constitutes a **practicable** timeframe to complete the measures that precede submitting an STR, FINTRAC may review:

- your previously submitted STRs, including their quality, timing and volume
- the nature of the original transaction
- the size of your business and your business model
- your internal processes and procedures
- the complexity of the transactions
- the number of relevant transactions identified in the STR
- the nature of the indicators and grounds for suspicion
- the facts of the case
- the overall number of transactions in your assessment
- other relevant considerations

FINTRAC's Assessment Manual³⁴⁸ and FINTRAC's guidance on "What is a suspicious transaction report?"³⁴⁹ provide additional and comprehensive information about their assessment process and areas of examination for the reporting of STRs.

³⁴⁷ FINTRAC, *What is a suspicious transaction report?*, August 12, 2021

³⁴⁸ FINTRAC, *FINTRAC Assessment Manual*, March 21, 2022

³⁴⁹ FINTRAC, *What is a suspicious transaction report?*, August 12, 2021

CHAPTER 10

Report receiving \$10,000 or more in cash or in virtual currency

If the funds received involve C\$10,000 or more in cash or in virtual currency in a “single transaction” (which may include multiple transactions) within a consecutive 24-hour window, a large cash transaction report (LCTR)³⁵⁰ or a large virtual currency transaction report (LVCTR) should be completed, retained and filed with FINTRAC.

If you report a LCTR no receipt of funds is necessary if you keep a copy of the LCTR. Since virtual currency are not defined as “funds” no receipt of funds is necessary, only the submission of the LVCTR and the retention of a copy is required.

Client identification must occur at or before the time the cash or virtual currency are received, although it should occur as soon as practical after being engaged to conduct a triggering activity. In instances where cash or virtual currency are received unexpectedly and without the client present, the accountant or accounting firm should identify the client prior to processing or returning the cash or virtual currency (both to meet regulatory obligations and to establish ownership over the property).

If an accountant or accounting firm authorizes another person or entity to receive funds or virtual currency on their behalf in connection with their triggering activities, and that other person or entity receives an amount of \$10,000 or more in cash or virtual currency in a single transaction in accordance with the authorization, the accountant or

³⁵⁰ FINTRAC, Transaction reporting guidance: [the 24-hour rule](#). May 4, 2021. Please note that FINTRAC has advised that from June 1st, 2021, these obligations will apply only to the reporting of large virtual currency transactions. The obligations will apply to large cash transactions, when FINTRAC updates the report forms for those transactions.

accounting firm has the obligation to keep the large cash transaction record or a large virtual currency transaction record as the accountant or accounting firm is deemed to have received the amount when it was received by the other person or entity.³⁵¹

10.1 The 24-hour rule³⁵²

The 24-hour rule is the requirement to aggregate multiple transactions when they total **\$10,000 or more within a consecutive 24-hour window** and the transactions are:³⁵³

- conducted by the same person or entity;
- conducted on behalf of the same person or entity (i.e., a third-party), or
- for the same beneficiary (person or entity)

For further clarity, as an example, when two or more cash transactions that total \$10,000 or more are conducted by the same person, on behalf of the same person, or for the same beneficiary, the 24-hour rule must be considered. However, if an amount under \$10,000 is received from a person, and then another amount under \$10,000 is received on behalf of that same person, and these amounts total \$10,000 but are not for the same beneficiary, then the 24-hour rule is not triggered. This is because both transactions are not received by the same person, nor are they received on behalf of the same person.

All transactions that total \$10,000 or more within a consecutive 24-hour window are to be reported to FINTRAC in a single report. This means that all transactions at or above the \$10,000 threshold that occur in the same 24-hour window must be included in the report and should not be reported separately.

The following can occur within a consecutive 24-hour window and must be reported in a single report under the 24-hour rule:

- several transactions in amounts under \$10,000 that total \$10,000 or more
- one transaction of \$10,000 or more
- several transactions in amounts under \$10,000 and one or more transactions of \$10,000 or more, or
- two or more transactions of \$10,000 or more

³⁵¹ PCMLTFR subsection 142(3)

³⁵² FINTRAC, *Transaction reporting guidance: the 24-hour rule*, May 4, 2021 Please note that FINTRAC has advised that from June 1st, 2021, these obligations will apply only to the reporting of large virtual currency transactions.

The obligations will apply to large cash transactions, when FINTRAC updates the report forms for those transactions.
³⁵³ PCMLTFR subsections 126, 127, 128, 129, and 130

The 24 hours that make up the period must be consecutive. The period cannot exceed 24 hours. The 24-hour rule should be considered broadly across your business if you have multiple locations in Canada. When transactions that fall under the 24-hour rule occur at multiple locations across your business, they should be reported in a single report.

10.1.1 **Aggregation of transactions under the 24-hour rule**

To identify the transactions that need to be aggregated and reported under the 24-hour rule, you have to determine the beginning and the end of the 24-hour window. This window is called a **static 24-hour window**. For example, 9 a.m. Monday to 8:59 a.m. Tuesday.

You are not limited to one 24-hour window. You have the option of using different static 24-hour windows for different types of reports and for different business lines. For example, you may determine that for operational purposes or to capture core business as much as possible you will use a 12:00 a.m. Monday to 11:59 p.m. Monday static 24-hour window, but for a specific business line you choose to use a different 24-hour window, for example, 8 p.m. Monday to 7:59 p.m. Tuesday.

Each transaction that falls under the 24-hour rule within a static 24-hour window will have to be viewed independently from the previous or subsequent static 24-hour window. Meaning that one transaction cannot fall under the 24-hour rule in multiple 24-hour windows. However, it is important to note that while you will monitor transactions for the applicability of the 24-hour rule within a static 24-hour window, you must also monitor all transactions, regardless of the static 24-hour window, to identify suspicious transactions that could relate to money laundering (ML) or terrorist activity financing (TF).

Your policies and procedures must include the time when your 24-hour windows begin and end. You will also need to indicate the times that your 24-hour window begins and ends in a mandatory field when you submit a report to FINTRAC.

10.1.2 **Application of the 24-hour rule to LCTRs and LVCTRs³⁵⁴**

Accountants and accounting firms have the obligation to report large cash transactions and large virtual currency transactions to FINTRAC in accordance with the 24-hour rule when:³⁵⁵

³⁵⁴ FINTRAC, *Transaction reporting guidance: the 24-hour rule*, May 4, 2021
³⁵⁵ PCMLTFR section 126

- **two or more** amounts in cash or virtual currency are received totalling \$10,000 or more within a static 24-hour window, and they **know** that those transactions:
 - were conducted by the same person or entity
 - were conducted on behalf of the same person or entity (third-party), or
 - are for the same beneficiary (person or entity)

10.2 Receiving funds of \$10,000 or more in cash

When you receive an amount of C\$10,000 or more in cash over one or more transactions over 24 consecutive hours (the 24-hour rule), in respect of a triggering activity, by, or on behalf of, the same person or entity, or the amounts are for the same beneficiary,³⁵⁶ you must (a) keep an LCTR (or in lieu, keep a copy of the LCTR³⁵⁷); (b) file an LCTR with FINTRAC within 15 days after the transaction; and (c) take reasonable measures to determine whether there is third-party involvement.

While an accountant or accounting firm might prohibit the acceptance of cash by policy or practice, cash may still be received inadvertently (by mail or otherwise). As a consequence, it is advisable to adopt a policy and procedure to deal with that eventuality. Some firms have adopted a policy whereby the sender will be invited to identify themselves to the firm in person and retrieve the funds intact within a certain number of days following receipt and notified that the funds will be returned intact otherwise by the same method by which they were received. Depositing the funds into the accountant's or accounting firm's account and then remitting them back to the sender may assist in achieving money laundering objectives, given the apparent legitimacy of payments received from an accountant/accounting firm. It has been the administrative practice of FINTRAC that obligations described below still apply if the funds are returned, since the cash has been received.

10.2.1 Exceptions for LCT record keeping and LCT reports

Exceptions to LCT record keeping.³⁵⁸ An accountant or accounting firm must keep a large cash transaction record for every amount of \$10,000 or more in cash that they receive in a single transaction in respect of triggering

³⁵⁶ PCMLTFR section 126

³⁵⁷ FINTRAC, *Record keeping requirements for accountants*, August 4, 2020. So long as all of the information that would otherwise be kept in the large cash transaction record is captured within the report. Any requirement related to keeping the large cash transaction record would still apply, such as verifying identity.

³⁵⁸ PCMLTFR section 50

activities unless the amount is received from a financial entity or public body or from a person who is acting on behalf of a client that is a financial entity or public body.

Exceptions to LCT reporting.³⁵⁹ Accountants and accounting firms are not required to make a large cash transaction report to FINTRAC if the cash is received from a financial entity or a public body. In this context, a financial entity means any of the following:

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

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

- a Canadian provincial or federal department or Crown agency
- an incorporated Canadian municipal body (including an incorporated city, town, village, metropolitan authority, district, county, etc.);
- a hospital authority – an organization that operates a public hospital and that is designated to be a hospital authority for GST/HST purposes. For more information on the designation of hospital authorities, refer to Canada Revenue Agency’s GST/HST Memorandum 25.2.³⁶⁰

10.3 Receiving \$10,000 or more in virtual currency

When you receive an amount of C\$10,000 or more in virtual currency³⁶¹ over one or more transactions over 24 consecutive hours (the 24-hour rule), in respect of a triggering activity, by, or on behalf of, the same person or entity, or the amounts are for the same beneficiary, you must (a) keep a LVCTR (or in lieu, keep a copy of the LVCTR); (b) file a LVCTR with FINTRAC within five working days after the day on which you receive the amount; and (c) take reasonable measures to determine whether there is third-party involvement.

³⁵⁹ FINTRAC, *Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically*, June 1, 2021

³⁶⁰ Canada Revenue Agency, *Designation of Hospital Authorities*, March 2009

³⁶¹ PCMLTFR subsection 129(1) and (2)

10.3.1 Exceptions for LVCT record keeping and LVCT reporting

Exceptions for LVCT record keeping.³⁶² An accountant or accounting firm must keep a LVCTR for every amount of \$10,000 or more in virtual currency that they receive in a single transaction in respect of triggering activities unless the amount is received from a financial entity or public body or from a person who is acting on behalf of a client that is a financial entity or public body.

Exceptions to LVCT reporting. You do not have to submit a LVCTR when you receive two or more amounts of virtual currency for the same beneficiary, if the amounts are each individually equivalent to less than \$10,000, but together total an amount equivalent to \$10,000 or more under the 24-hour rule, if the beneficiary is:³⁶³

- a public body
- a corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act and that operates in a country that is a member of the FATF, or
- an administrator of a pension fund that is regulated under federal or provincial legislation

You cannot apply this exception to amounts of virtual currency received for one of these beneficiaries under the 24-hour rule, if one or more of the amounts is individually equivalent to \$10,000 or more. In this scenario you must submit a separate LVCTR to FINTRAC for each amount that is individually equivalent to \$10,000 or more, as the reporting threshold has been met with the individual transaction.

10.3.2 Examples applied to LVCTRs and the 24-hour rule³⁶⁴

Assumptions for the scenarios below:

- the reporting entity is a money service business (MSB) that deals in virtual currency (VC) and is subject to the PCMLTFA and associated regulations
- the MSB's static window for their LVCTR process under the 24-hour rule is from 12:00 p.m. to 11:59 a.m. the following day
- the exchange rate for the VC is 1 for C\$1,000

³⁶² PCMLTFR section 51

³⁶³ PCMLTFR paragraphs 129(2)(a) to (c)

³⁶⁴ These scenarios are sourced from FINTRAC, *Transaction reporting guidance: the 24-hour rule*, May 4, 2021.

Scenario 1 — Receipt of virtual currency - 24-hour rule — Aggregation on the beneficiary

Description:

- Monday at 1:15 p.m., MSB receives 6 VC (equivalent to \$6000) from Ms. Red to be added to Mr. Blue's VC wallet.
- Monday at 5:08 p.m., MSB receives 3 VC (equivalent to \$3000) from Mr. Green to be added to Mr. Blue's VC wallet.
- Tuesday at 7:39 a.m., MSB receives 4 VC (equivalent to \$4000) from Mrs. White to be added to Mr. Blue's VC wallet.

LVCTR requirement

In this scenario, the MSB would submit an LVCTR under the 24-hour rule that combines the three transactions totalling an amount equivalent to \$13,000 based on the beneficiary, which is Mr. Blue.

Scenario 2 — Receipt of virtual currency - 24-hour rule — Aggregation on the conductor

Description:

- Wednesday at 4:20 p.m., MSB receives 2 VC (equivalent to \$2000) from Mrs. White to be added to Mr. Blue's VC wallet.
- Wednesday at 11:08 p.m., MSB receives 4 VC (equivalent to \$4000) from Mrs. White to be added to Mr. Green's VC wallet.
- Thursday at 3:39 a.m., MSB receives 6 VC (equivalent to \$6000) from Mrs. White to be added to Ms. Red's VC wallet

LVCTR requirement

In this scenario, the MSB would submit an LVCTR under the 24-hour rule that combines the three transactions totalling an amount equivalent to \$12,000 based on the conductor, which is Mrs. White.

Scenario 3 — Receipt of virtual currency - 24-hour rule — Aggregation on the third-party

Description:

- Friday at 12:12 p.m., MSB receives 8 VC (equivalent to \$8000) from Mrs. White to be added to Mr. Blue's VC wallet. The MSB knows that Mrs. White conducted the transaction on behalf of Ms. Red.

- Saturday at 11:32 a.m., MSB received 4 VC (equivalent to \$4000) from Mr. Blue to be added to Mrs. White's VC wallet. The MSB knows that Mr. Blue conducted the transaction on behalf of Ms. Red.

LVCTR requirement

In this scenario, the MSB would submit an LVCTR under the 24-hour rule that combines the two transactions totalling an amount equivalent to \$12,000 based on the third-party, which is Ms. Red.

10.4 General exceptions

If you are required to keep a record with information that is readily available in other records, you do not have to record the information again.³⁶⁵

You are **not required to keep a LCTR, LVCTR or a receipt of funds record** if the cash, virtual currency or funds is received from a client that is a financial entity or a public body, or from a person who is acting on behalf of a client that is a financial entity or public body.³⁶⁶

You are **not required to keep a receipt of funds record** if the funds are received from a public body, a very large corporation or trust, or a subsidiary of those entities, if the financial statements of the subsidiary are consolidated with those of the public body, or very large corporation or trust.

10.5 Verifying the identity of clients

You must verify the identity of persons and entities when you receive \$10,000 or more in cash or virtual currency. See Chapters 23 and 24 respectively for all requirements relating to the verification of identity of a person and of an entity.

³⁶⁵ PCMLTFR section 153 - A person or entity that is required to keep a record under these Regulations is not required to include information in that record that is readily obtainable from other records that they are required to keep under these Regulations.

³⁶⁶ PCMLTFR sections 50, 51 and paragraph 52(a) and FINTRAC, *Record keeping requirements for accountants*, August 4, 2021

10.6 Keep records

You must have the information recorded in your system that can satisfy a request by FINTRAC, or examination purposes, within 30 days after the day of the request³⁶⁷. Table 9 describes the records to be kept for a LCTR and LVCTR (if applicable).

Table 9

Records to keep (if applicable)	Receiving C\$10,000 or more in cash OR Receiving C\$10,000 or more in virtual currency
<i>RECORDS</i>	<i>REQUIREMENT</i>
1. Keep a receipt of funds record	When an accountant or accounting firm engages in a triggering activity, the AML/ATF legislation requires that a receipt of funds record be completed for every amount of C\$3,000 or more of funds (in cash or in another form) in the course of a single transaction. However, the definition of funds does not include virtual currency . ³⁶⁸ See Section 8.1 and general exceptions in Section 10.4 of this guide.
2. Keep a record of verification of the identity of the person, the identity of the corporation or the entity other than a corporation	You must verify the identity of persons and entities when you receive \$10,000 or more in cash or virtual currency. See Section 8.2 and Chapters 23 and 24 respectively for all requirements relating to the verification of identity of a person and of an entity.
3. Keep a business relationship record ³⁶⁹ (If applicable)	If you have a business relationship, you must keep a record that sets out: the purpose and intended nature of the business relationship, and the measures taken: a) when you conduct ongoing monitoring of the business relationship, and b) of the information obtained from that ongoing monitoring. ³⁷⁰ See Section 26.1.2.

³⁶⁷ PCMLTFR section 149

³⁶⁸ PCMLTFR subsection 1(2)

³⁶⁹ See PCMLTFR paragraph 4.1 (b). An Accountant or Accounting Firm enters into a business relationship the second time they are required to verify the identity of the client.

³⁷⁰ PCMLTFR subsection 146(1)

Records to keep (if applicable)	Receiving C\$10,000 or more in cash OR Receiving C\$10,000 or more in virtual currency
RECORDS	REQUIREMENT
4. Keep a business relationship and ongoing monitoring record (if applicable)	<p>If you have a business relationship, you have ongoing obligations³⁷¹ to periodically monitor the business relationship and keep an ongoing business relationship record (see Section 26.1.2 Sample - Record of business relationship and ongoing monitoring Information),³⁷² recording the measures taken when you conduct ongoing monitoring of the business relationship with that person or entity and of the information obtained from that ongoing monitoring on a risk-sensitive basis, for the purpose of:³⁷³</p> <ul style="list-style-type: none"> • detecting any reportable suspicious transactions or attempted suspicious transactions • keeping client identification information up to date • reassessing the level of risk associated with the client's transactions and activities • determining whether transactions or activities are consistent with the information obtained about the client, including the risk assessment of the client
5. Keep a record of reasonable measures to confirm the accuracy of beneficial ownership information (if applicable)	<p>If your client is an entity, at the time you verify the identity of an entity, you must also obtain information about its beneficial ownership.³⁷⁴ If you established a business relationship with that client, you must also confirm the accuracy of the beneficial ownership information in the course of ongoing monitoring. See Section 8.4.</p> <p>If your client is an entity, and if you are unable to obtain beneficial ownership information, to keep it up to date in the course of ongoing monitoring of business relationships or to confirm its accuracy, you must take reasonable measures to verify the identity of the entity's chief executive officer or the person who performs that function; and take special measures (enhanced measures) referred to in section 157 of the PCMLTFR which are:</p> <ol style="list-style-type: none"> a. taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity b. taking any other enhanced measure to mitigate the risks, including <ol style="list-style-type: none"> i. ensuring, at a frequency appropriate to the level of risk, that client identification information and beneficial information is up to date ii. conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships to: <ol style="list-style-type: none"> a. detect suspicious transactions b. keep client identification information, beneficial ownership and business relationship information up to date c. reassessing the level of risk associated with the client's transactions and activities d. determining whether transactions or activities are consistent with the information obtained about their client, including the risk assessment of the client

371 PCMLTFR section 123.1

372 PCMLTFR section 146(1)

373 PCMLTFR section 123.1

374 PCMLTFR subsection 138(1)

Records to keep (if applicable)	Receiving C\$10,000 or more in cash OR Receiving C\$10,000 or more in virtual currency
<i>RECORDS</i>	<i>REQUIREMENT</i>
6. Keep record of third-party determination for large cash/ large virtual currency transaction	You must take, upon receipt of the cash or virtual currency, reasonable measures to determine whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party. See Section 32.1 of this guide for more information.
7. Keep record of grounds to suspect third-party involvement for large cash/ large virtual currency transactions	If you are not able to determine ³⁷⁵ whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party but there are reasonable grounds to suspect that they are, you must keep a record that (a) indicates whether, according to the person from whom the cash or virtual currency is received, they are acting on their own behalf only; and (b) describes the reasonable grounds to suspect that they are acting on behalf of a third-party. See Sections 32.1 and 32.2 of this guide.
8. Keep large cash transaction record	If you keep a copy of the large cash transaction report, there is no need to create a large cash transaction record.
9. Keep copy of large cash transaction report	You must keep a copy of the large cash transaction report. By doing so you do not need to keep a large cash transaction record. See Chapter 27 for a sample of the large cash transaction report form.
10. Keep large virtual currency transaction record	If you keep a copy of the large virtual currency transaction report, there is no need to create a large virtual currency transaction record.
11. Keep copy of large virtual currency transaction report	You must keep a copy of the large virtual currency transaction report. By doing so you do not need to keep a large virtual currency transaction record. See Chapter 28 for a sample of the large virtual currency transaction report form.
12. Keep PEP, HIO, family and close associate record when receiving \$100,000 or more in cash or virtual currency	If you receive an amount of \$100,000 or more, in cash or in virtual currency, you must take reasonable measures to determine whether a person from whom you received this amount is a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a family member of, or a person who is closely associated with, one of those persons. ³⁷⁶ See Section 10.9 of this guide.

375 PCMLTFR subsection 134(3)

376 PCMLTFR subsection 120.1(3)

10.7 What is a large virtual currency transaction record?

In the case of accountants and accounting firms, a large virtual currency transaction³⁷⁷ record means a record that indicates the receipt of an amount of \$10,000 or more in virtual currency in a single transaction (in compliance with the 24-hour rule) and that contains the following information:

- a. the date of the receipt
- b. if the amount is received for deposit into an account, the name of each account holder
- c. the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth
- d. the type and amount of each virtual currency involved in the receipt
- e. the exchange rates used and their source
- f. the number of every other account that is affected by the transaction, the type of account and the name of each account holder
- g. every reference number that is connected to the transaction and has a function equivalent to that of an account number
- h. every transaction identifier, including the sending and receiving addresses

³⁷⁷ PCMLTFR section 1(2)

Table 10*Sample large virtual currency transaction record*

LARGE VIRTUAL CURRENCY TRANSACTION RECORD			
The following information must be collected, retained and recorded for each prescribed transaction where the organization receives virtual currency with a value of CAD \$10,000 or more from a client in a single transaction in respect of triggering activities.			
INFORMATION ON THE PERSON FROM WHOM YOU RECEIVED THE VIRTUAL CURRENCY			
Last name		First name	
Street address			Apartment/Unit #
City	Prov.	Postal code	
Date of birth	Nature of principal business or occupation		
INFORMATION WHEN AMOUNT IS RECEIVED FROM OR ON BEHALF OF AN ENTITY			
Name of entity		Nature of principal business	
Street address			Apartment/Unit #
City	Prov.	Postal code	
INFORMATION ON ALL OTHER PERSONS INVOLVED IN THE TRANSACTION			
Last name		First name	
Street address			Apartment/Unit #
City	Prov.	Postal code	
Date of birth	Nature of principal business or occupation		
INFORMATION ON ALL OTHER ENTITIES INVOLVED IN THE TRANSACTION			
Last name		First name	
Street address			Apartment/Unit #
City	Prov.	Postal code	
TRANSACTION INFORMATION			
Date of the receipt		Amount	
Type of each virtual currency		Amount of each virtual currency	
If applicable, exchange rate		If applicable, source of exchange rate	
TRANSACTION IDENTIFIER			
Provide every transaction identifier		Sending addresses:	
		Receiving addresses	

INFORMATION ON EVERY ACCOUNT AFFECTED BY THE TRANSACTION, IF APPLICABLE	
Account #	Type of account
Accountholder's full name	
Every reference number connected to the transaction that is equivalent to account number	
RECORD TO KEEP	
If the receipt of a large virtual currency transaction is about a corporation, you also need to keep a copy of the part of the official corporate records showing the provisions relating to the power to bind the corporation regarding the transaction.	

10.7.1 Exception for large virtual currency transaction record

The AML/ATF legislation³⁷⁸ clarifies for greater certainty that keeping a record of a large virtual currency transaction in respect of every amount of \$10,000 or more in virtual currency that you receive in a single transaction does not apply to:

- a. a transfer or receipt of virtual currency as compensation for the validation of a transaction that is recorded in a distributed ledger
- b. an exchange transfer or receipt of a nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information

The AML/ATF legislation³⁷⁹ defines for the purpose of this section, that a distributed ledger means a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities.

10.8 What is a large cash transaction record?

In the case of accountants and accounting firms, a large cash transaction record means a record that indicates the receipt of an amount of \$10,000 or more in cash in a single transaction (in compliance with the 24-hour rule) and that contains the following information:

³⁷⁸ PCMLTFR subsection 151(1)
³⁷⁹ PCMLTFR subsection 151(2)

1. the date of the receipt
2. if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours
3. the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth
4. the type and amount of each fiat currency involved in the receipt
5. the method by which the cash is received
6. if applicable, the exchange rates used and their source
7. the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. every reference number that is connected to the transaction and has a function equivalent to that of an account number
9. the purpose of the transaction

The sample form in Table 11, Section 10.8.1, may be used.

10.8.1 Sample large cash transaction record

Table 11

Sample large cash transaction record

LARGE CASH TRANSACTION RECORD			
The following information must be collected, retained and recorded for each prescribed transaction where the organization receives cash with a value of CAD \$10,000 or more from a client in a single transaction in respect of triggering activities.			
INFORMATION ON THE PERSON FROM WHOM YOU RECEIVED THE CASH			
Last name		First name	
Street address			Apartment/Unit #
City	Prov.	Postal code	
Date of birth	Nature of principal business or occupation		
INFORMATION WHEN AMOUNT IS RECEIVED FROM OR ON BEHALF OF AN ENTITY			
Name of entity		Nature of principal business	
Street address			Apartment/Unit #
City	Prov.	Postal code	

INFORMATION ON ALL OTHER PERSONS INVOLVED IN THE TRANSACTION		
Last name		First name
Street address		Apartment/Unit #
City	Prov.	Postal code
Date of birth	Nature of principal business or occupation	
INFORMATION ON ALL OTHER ENTITIES INVOLVED IN THE TRANSACTION		
Name of entity		Nature of principal business
Street address		Apartment/Unit #
City	Prov.	Postal code
TRANSACTION INFORMATION		
Date of the receipt		Amount
Type of each fiat currency		Amount of each fiat currency
If applicable, Exchange Rate		If applicable, source of exchange rate
Purpose, details and type of transaction		Other persons or entities involved
Method by which amount received		
TRANSACTION IDENTIFIER		
Provide every transaction identifier		Sending addresses:
		Receiving addresses
INFORMATION ON EVERY ACCOUNT AFFECTED BY THE TRANSACTION, IF APPLICABLE		
Account #		Type of account
Accountholder's full name		
Every reference number connected to the transaction that is equivalent to account number		
RECORD TO KEEP		
If the receipt of a large cash transaction is about a corporation, you also need to keep a copy of the part of the official corporate records showing the provisions relating to the power to bind the corporation regarding the transaction.		

10.9 Receiving \$100,000 or more in cash or virtual currency

If you receive an amount of \$100,000 or more, in cash or in virtual currency, you must, within 30 days after the day on which the transaction is conducted, take reasonable measures to determine whether a person from whom you received this amount, is a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a

family member of, or a person who is closely associated with, one of those persons.^{380 381} As a reminder from the glossary in the guide and a FINTRAC FAQ,³⁸² here are relevant definitions:

Close associate of a politically exposed domestic person, a politically exposed foreign person or a head of an international organization is not defined in the AML/ATF legislation. FINTRAC provides in its guidance³⁸³ some examples that are useful in making such a determination. Some examples of a close association for personal or business reasons include a person who is: business partners with, or who beneficially owns or controls a business with, a PEP or HIO; in a romantic relationship with a PEP or HIO; involved in financial transactions with a PEP or a HIO; a prominent member of the same political party or union as a PEP or HIO; serving as a member of the same board as a PEP or HIO; or closely carrying out charitable works with a PEP or HIO. FINTRAC's guidance; or are listed as joint on a policy where one of the holders may be a PEP or HIO. FINTRAC's guidance should be consulted.

Family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is (a) their spouse or common-law partner; (b) their child; (c) their mother or father; (d) the mother or father of their spouse or common-law partner; or (e) a child of their mother or father.

Head of an international organization³⁸⁴ means a person who, at a given time, holds – or has held within five years before that time³⁸⁵ – the office or position of head of an international organization that is established by the governments of states or the head of an institution of any such organization; or an international sports organization.

Politically exposed domestic person³⁸⁶ means a person who, at a given time, holds – or has held within five years before that time³⁸⁷ – one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or the office or position referred to in paragraphs (b) and (k) in a municipal government: (a) Governor General, lieutenant governor or head of government; (b) member

380 PCMLTFR subsection 120.1(3)

381 PCMLTFR subsection 122.1(6)

382 FINTRAC, *Frequently asked questions about domestic politically exposed persons and heads of international organizations*, June 1, 2021

383 FINTRAC, *Politically exposed persons and heads of international organizations guidance*, December 15, 2021

384 PCMLTFA subsection 9.3(3)

385 PCMLTFR subsection 2(2)

386 PCMLTFA paragraph 9.3(3)

387 PCMLTFR subsection 2(2)

of the Senate or House of Commons or member of a legislature; (c) deputy minister or equivalent rank; (d) ambassador, or attaché or counsellor of an ambassador; (e) military officer with a rank of general or above; (f) president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province; (g) head of a government agency; (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada; (i) leader or president of a political party represented in a legislature; (j) holder of any prescribed office or position; or (k) mayor.

Politically exposed foreign person³⁸⁸ means a person who holds or has held one of the following offices or positions in or on behalf of a foreign state: (a) head of state or head of government; (b) member of the executive council of government or member of a legislature; (c) deputy minister or equivalent rank; (d) ambassador, or attaché or counsellor of an ambassador; (e) military officer with a rank of general or above; (f) president of a state-owned company or a state owned bank; (g) head of a government agency; (h) judge of a supreme court, constitutional court or other court of last resort; (i) leader or president of a political party represented in a legislature; or (j) holder of any prescribed office or position.

10.9.1 **What are the reasonable measures you must take to determine if the person is a politically exposed person, a head of an international organization, their family member or a close associate?**

“Reasonable measures” mean that you must take steps to collect certain information, even if taking those steps did not result in the desired information being obtained. For example, according to FINTRAC Guidance³⁸⁹ this can include doing one or more of the following: asking the client, conducting open-source searches, or consulting commercially available information.

³⁸⁸ PCMLTFA paragraph 9.3(3)

³⁸⁹ FINTRAC, *Guidance Glossary*, May 4, 2021

10.9.2 If I have made such a determination, now what?³⁹⁰

10.9.2.1 Receipt of \$100,000 In cash or virtual currency from a politically exposed foreign person, their family member or a close associate

Use Table 12A in this section to identify the requirements an accountant or accounting firm must meet if it has been determined that the person from whom you have received \$100,000 or more in cash or virtual currency is a **politically exposed foreign person**, their family member or a close associate. In such a case, you must:

- take reasonable measures to establish the source of cash or virtual currency used for that transaction³⁹¹
- determine the source of the person's wealth
- ensure that a member of senior management reviews the transaction³⁹²

³⁹⁰ FINTRAC, *Politically exposed persons and heads of international organizations guidance for non-account-based reporting entity sectors*, June 11, 2021

³⁹¹ PCMLTFR subsection 120.1(3) and paragraphs 122.1(2)(a) and (b)

³⁹² FINTRAC, *Politically exposed persons and heads of international organizations guidance for non-account-based reporting entity sectors*, June 11, 2021

Table 12A

\$100,000 or more in cash or virtual currency received from a foreign PEP, or family member or close associate

Requirement if you receive \$100,000 or more in cash or virtual currency from a Foreign PEP, family member or close associate	Records to keep	Regulatory references
<p>Once you determine that the person is a politically exposed foreign person, or a family member of, or a person who is closely associated with, that person you must:</p> <ul style="list-style-type: none"> a. take reasonable measures to establish the source of the cash or virtual currency used for the transaction and the source of the person's wealth; b. ensure that a member of senior management reviews the transaction 	<p>If senior management reviews this transaction you must keep a record of³⁹³:</p> <ul style="list-style-type: none"> a. the office or position and the organization or institution in respect of which the person is determined to be a PEPF, or a family member of, or a person who is closely associated with, a PEPF b. the date of the determination c. the source, if known, of the funds or virtual currency used for the transaction d. the source, if known, of the person's wealth e. the name of the member of senior management who reviewed the transaction f. the date of that review <p>In the case of family members and close associates of PEPFs, you may also want to include in the record the nature of the relationship between the person and the PEPF, as applicable.</p> <p>Retention: If you review a prescribed PEPF transaction, then you must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR Subsections 120.1(3), 122.1(6) paragraphs 122.1(2) (a) and (b), subsection 123(5) and paragraph 148(1)(c)</p>

393 PCMLTFR subsection 123(5)

10.9.2.2 *Receipt of \$100,000 in cash or virtual currency from a politically exposed domestic person, head of an international organization or family member or close associate*

Use Table 12B in this section to identify the requirements an accountant or accounting firm must meet if it has been determined that the person from whom you have received \$100,000 or more in cash or virtual currency is a **PEDP, HIO** or family member or close associate of a domestic PEP or HIO **and** consider, based on your risk assessment, that there is a **high risk** of the person being involved in an ML/TF offence. In such a case, you must:

- take reasonable measures to establish the source of the funds or virtual currency used for that transaction
- determine the source of the person's wealth
- ensure that a member of senior management reviews the transaction

Table 12B

\$100,000 or more received in cash or virtual currency from a domestic PEP, HIO, or family member or close associate

Requirement if you receive \$100,000 or more in cash or virtual currency from a domestic PEP, HIO, or family member or close associate	Records to keep	Regulatory references
<p>Once you determined a person is a PEDP, HIO, or a family member of one of those persons, or person who is closely associated with a PEDP or a HIO and you consider, based on your risk assessment (see subsection 9.6(2) of the PCMLTFA), that there is a high risk of a money laundering offence or terrorist activity financing offence, you must:</p> <ul style="list-style-type: none"> a. take reasonable measures to establish the source of the cash or virtual currency used for the transaction and the source of the person's wealth b. ensure that a member of senior management reviews the transaction 	<p>If senior management reviews this transaction you must keep a record of:³⁹⁴</p> <ul style="list-style-type: none"> a. the office or position and the organization or institution in respect of which the person is determined to be a politically exposed domestic person or a head of an international organization, or a family member of, or a person who is closely associated with, one of those persons b. the date of the determination c. the source, if known, of the funds or virtual currency used for the transaction d. the source, if known, of the person's wealth e. the name of the member of senior management who reviewed the transaction f. the date of that review <p>In the case of family members and close associates of PEDPs and HIOs, you may also want to include in the record the nature of the relationship between the person and the PEDP or HIO, as applicable.</p> <p>Retention: If you review a prescribed PEDP or HIO transaction, then you must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 120.1(3), 122.1(6), subsection 123(5), subsection 122.1(4), and paragraph 148(1)(c).</p>

394 PCMLTFR subsection 123(5)

10.9.3 Exceptions

You do not have to make a PEP or family member determination if you already determined that a person is a foreign PEP or a family member of a foreign PEP.³⁹⁵

You do not need to determine if a person is a PEP, HIO or a family member or close associate of a PEP or HIO, as applicable, or keep the related records for the following:³⁹⁶

- a public body
- a very large corporation or trust, or
- a subsidiary of those entities, if the financial statements of the subsidiary are consolidated with those of the public body, very large corporation or trust

³⁹⁵ PCMLTFR subsection 155(4)
³⁹⁶ PCMLTFR subsection 154(2)

CHAPTER 11

Reporting terrorist property

The AML/ATF legislation requires, in addition to making a terrorist property report (TPR) to FINTRAC, a requirement under the Criminal Code and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST) for anyone in Canada and any Canadian outside Canada to disclose, to the Royal Canadian Mounted Police (RCMP)³⁹⁷ and the Canadian Security Intelligence Service (CSIS),³⁹⁸ the existence of property that they **know** is owned or controlled by or on behalf of a terrorist, a terrorist group or **believe** that property in their possession is owned or controlled by a listed person.³⁹⁹

While accountants and accounting firms have the obligation to submit a TPR to FINTRAC under the AML/ATF legislation, this obligation is triggered when you are required to make a disclosure under subsection 83.1 of the Criminal Code or section 8 of RIUNRST.⁴⁰⁰

It is therefore important to familiarize yourself with your Criminal Code and RIUNRST obligations in order to be able to comply with your TPR obligations under the AML/ATF legislation. As required by the Criminal Code or the RIUNRST, you may also have additional activities associated to these obligations. Further, you may be subject to additional obligations regarding terrorist groups, listed persons and other sanctioned individuals and entities (known as “designated persons”).

These obligations fall outside of the scope of the AML/ATF legislation and is **not addressed** in this guide or in FINTRAC’s guidance. More information with respect to these obligations can be found under various Canadian statutes and regulations.

³⁹⁷ Royal Canadian Mounted Police, [National Security Information Network](#), December 21, 2020

³⁹⁸ Government of Canada, [Reporting National Security Information](#), October 10, 2019

³⁹⁹ FINTRAC, [Reporting terrorist property to FINTRAC](#), August 4, 2021

⁴⁰⁰ PCMLTFA subsection 7.1(1)

11.1 Knowledge or belief of terrorist property

Two situations can trigger the requirement to send a TPR to FINTRAC.

1. knowing that property is owned or controlled by or on behalf of a terrorist or a terrorist group
2. believing that property is owned or controlled by or on behalf of a listed person

As an accountant or an accounting firm, you have to send a TPR to FINTRAC if you have property in your possession or control that you **know is owned or controlled by or on behalf of a terrorist or a terrorist group** and if you have property in your possession or control that you **believe is owned or controlled by or on behalf of a listed person**. In both situations, this includes information about any transaction or proposed transaction relating to that property.

11.2 Definitions⁴⁰¹

Property: Property is anything owned or controlled by a person or entity, whether tangible or intangible. It includes real and personal property, as well as deeds and instruments that give a title or right to property, or to receive money or goods. It also includes any property that has been converted or exchanged or acquired from any conversion or exchange.

The following are examples of property for the purpose of a TPR:

- cash
- monetary instruments (for example, cheques, bank drafts or money orders)
- casino products and tokens
- virtual currency
- accounts (for example, personal or business accounts, Registered Retirement Savings Plans [RRSP], Tax-Free Savings Accounts [TFSA])
- prepaid payment products and accounts
- securities (for example, stocks, bonds or mutual funds)
- jewellery, precious metals or precious stones
- real estate, including an instrument that gives title or right to a property (for example, a deed)
- insurance policies

⁴⁰¹ FINTRAC, *Reporting terrorist property to FINTRAC*, August 4, 2021

Terrorist group: Under subsection 83.1(1) of the Criminal Code, **every person in Canada** and **every Canadian outside Canada** must disclose without delay to the commissioner of the **Royal Canadian Mounted Police (RCMP)** or **to the director of the Canadian Security Intelligence Service (CSIS)** the existence of property in their possession or control that they know is owned or controlled by or on behalf of a **terrorist group**. . In addition, you must disclose, to the RCMP or CSIS, information about any transaction or proposed transaction in respect of that property. According to subsection 83.1(1) of the Criminal Code, a **terrorist group** is defined as:

- an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity
- a **listed entity**, or
- an association of such entities

Listed entity: According to subsection 83.01(1) of the Criminal Code, a listed entity is one that appears on a list established under section 83.05 of the Criminal Code. This list is a public means of identifying a group or individuals as being associated with terrorist activity. You can consult this list on the Public Safety Canada website.⁴⁰² An entity for these purposes could include a person, group, trust, partnership or fund, or an unincorporated association or organization.

Listed person: Under subsection 8(1) of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST), every person in Canada, every Canadian outside Canada, and certain prescribed entities must disclose without delay to the commissioner of the RCMP or the director of CSIS the existence of property in their possession or control that they have reason to believe is owned, held or controlled by or on behalf of a listed person. In addition, you must also disclose, to the RCMP or CSIS, information about a transaction or proposed transaction in respect of such property.

According to sections 1 and 2(1) of the RIUNRST, a listed person is an individual or entity that is listed in the schedule of the RIUNRST because there are reasonable grounds to believe that the individual or entity:

- has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity
- is controlled directly or indirectly by any such individual or entity, or

⁴⁰²Public Safety Canada, [Currently listed entities](#)

- is acting on behalf of, or at the direction of, or in association with any such individual or entity

You can consult the list by viewing the schedule in the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*.⁴⁰³

FINTRAC advises that:

- The information you disclose to the RCMP or CSIS, or report to your provincial or federal regulator (if applicable, as required by the Criminal Code or the RIUNRST) should be consistent with the information you submit to FINTRAC in a TPR.
- Under the Criminal Code and RIUNRST, if you know that a transaction is related to property owned or controlled by or on behalf of a terrorist group or listed person, **you should not complete it**.⁴⁰⁴

11.3 Requirements

It is an offence to deal with property when you have knowledge or belief of terrorist property or a listed person, and imperative that it be **reported immediately to FINTRAC, the RCMP and CSIS**. The AML/ATF legislation does not impose a duty on accountants or accounting firms to screen the names of their triggering activities clients against terrorist lists. An accountant or accounting firm may, for example through the course of normal business activities, come across information that leads to determine that a client is associated with or is part of a terrorist group. This can occur when you come across: publicly available information or media articles stating that your client has carried out or facilitated terrorist activity; or official, publicly available lists relating to terrorist activity (for example, the Office of Foreign Assets Control (OFAC) and European Union (EU) lists).

TPRs differ from other reports that are submitted to FINTRAC because a transaction or attempted transaction does not have to occur for you to submit a TPR. Instead, it is the mere existence of property (such as a bank account) owned or controlled by or on behalf of a terrorist group or listed person that prompts your obligation to submit a TPR.

⁴⁰³Public Safety Canada, [Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism \(SOR/2001-360\)](#), March 7, 2022

⁴⁰⁴FINTRAC, [Reporting terrorist property to FINTRAC](#), November 19, 2021

TPRs contribute to Canada's anti-money laundering (AML) and anti-terrorist financing (ATF) regime as they provide information about property held by a terrorist group or a listed person that may not be found in other financial transaction reports. In addition, through FINTRAC's tactical analysis, TPRs can provide invaluable insight and assist in the detection of individuals and entities that may be involved in terrorist activity financing networks.

11.3.1 **Knowing about a terrorist or a terrorist group**

Once you know that any property in your possession or control is owned or controlled by or on behalf of a terrorist or a terrorist group, or after any transaction is made or proposed for such a property, a terrorist property report must be sent to FINTRAC **immediately**. If you know 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 it**. This is because such property must be frozen under the Criminal Code. If you are not sure that you are dealing with a terrorist or terrorist group, but suspect that you might be, then a suspicious transaction report is required if a transaction was completed. You also have to complete a suspicious transaction report if the suspicious transaction was attempted.

11.3.2 **Believing that property is owned or controlled by or on behalf of a listed person**

You may have other information that leads you to believe that an individual or an entity is a listed person or associated with such a person. Once you believe that any property in your possession or control is owned or controlled by or on behalf of a listed person, or after any transaction is made or proposed for such a property, a terrorist property report must be sent to FINTRAC immediately and **you should not complete the transaction**. This is because such property must be frozen under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*.

11.3.3 **Suspicion that property is owned or controlled by or on behalf of a listed person**

If you are not sure that you are dealing with a listed person, but suspect that you might be, then an STR is required if a transaction was completed. You also must complete a suspicious transaction report if the suspicious transaction was attempted.

11.3.3.1 **Suspicious transaction report**

It is important to remember that you must submit an STR to FINTRAC if a transaction has taken place or was attempted and you have reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering (ML) offence or a terrorist activity financing (TF) offence.⁴⁰⁵

If a transaction was attempted or completed, and it involved property that you know is owned or controlled by or on behalf of a terrorist group, or that you believe is owned or controlled by or on behalf of a listed person (for which you must submit a TPR), you should also submit an STR to FINTRAC. This is because you have reached the threshold of reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence.

If you do not know or believe that the property in your possession or control is owned or controlled by or on behalf of a terrorist group or listed person, but you suspect that it is, then a TPR is not required. However, you must submit an STR to FINTRAC if there was an attempted or completed transaction associated with this property.

11.4 **Lists/Schedule of terrorists, terrorist groups, and listed persons**

Canada's listings of terrorists, terrorist groups, and listed persons are available on the Public Safety Canada website.⁴⁰⁶

Listed entities may be found on the Public Safety Canada website, under 'Currently listed entities.'⁴⁰⁷

Listed persons may be found in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism."⁴⁰⁸

⁴⁰⁵PCMLTFA section 7

⁴⁰⁶Public Safety Canada, [Currently listed entities](#)

⁴⁰⁷Ibid

⁴⁰⁸Public Safety Canada, [Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism \(SOR/2001-360\)](#), March 7, 2022

11.5 Filing a terrorist property report

You must submit TPRs to FINTRAC electronically **by fax** if you have the technical capability to do so. If you do not have the capability to submit by fax, you must send the report by mail.⁴⁰⁹ A TPR must now be sent “**immediately**” as opposed to what was previously required as “without delay.”

REMINDER: Concurrent with the filing of a TPR to FINTRAC, the accountant or accounting firm must send the information to the Royal Canadian Mounted Police (RCMP) and to the Canadian Security Intelligence Service (CSIS) immediately.⁴¹⁰

FINTRAC’s TPR form can be printed from its reporting web page⁴¹¹ or you can request a form to be faxed or mailed to you by calling FINTRAC at 1-866-346-8722.

The terrorist property report, included as Chapter 29 Appendix O – Terrorist Property Form, must be filed with FINTRAC immediately by faxing it to 1-866-226-2346. This form is also available from the FINTRAC website.⁴¹²

Submit a TPR by fax to: 1-866-226-2346

Submit a TPR by mail through regular or registered mail to:

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

There is no official acknowledgment of receipt when you submit a TPR to FINTRAC.

A copy of the TPR must be retained for five years following the transaction, and it is advisable to maintain a record of successful transmission of the fax. Instructions to complete the form are included on the pages following the form. All fields marked with an asterisk (*) are mandatory. All other fields are “reasonable measures”⁴¹³ fields, which mean that they must be completed if the information is available to the accountant or accounting firm. The requirement to report information set out in the STR and TPR does not

409 PCMLTFSTRR section 12

410 FINTRAC, [Reporting terrorist property to FINTRAC](#), June 1, 2021

411 FINTRAC, [Reporting forms](#), July 23, 2021

412 FINTRAC, [Terrorist property report form](#), June 2021

413 PCMLTFSTRR subsection 11(1) and (2) states “reasonable measures”

apply if the accountant or accounting firm believes that taking the reasonable measures to obtain the information would inform a person or entity that conducts or attempts or proposes to conduct a transaction with them that the transaction and related information will be reported as an STR or TPR (under section 7 or 7.1 of the PCMLTFA).⁴¹⁴

11.6 Keeping a record

As noted above, a copy of the TPR must be kept. The AML/ATF legislation requires that you keep a copy of all reports sent to FINTRAC.⁴¹⁵

11.7 Advising the RCMP and CSIS

Concurrent with the filing of a terrorist property report, the accountant or accounting firm must send the information to the RCMP and CSIS immediately.

414 PCMLTFSTRR subsection 11(1) and (2)
415 PCMLTFR section 144

CHAPTER 12

AML/ATF and privacy obligations

In Canada, accountants and accounting firms have both AML/ATF and privacy obligations. The use of personal information in Canadian commercial activities is protected by the Personal Information Protection and Electronic Documents Act (PIPEDA), or by similar provincial legislation. You have to inform clients about the collection of their personal information. However, you do not have to inform them when you include their personal information in the reports you are required to submit to FINTRAC. This means accountants and accounting firms must only collect personal information that you need.

The AML/ATF legislation requires certain information to be collected by reporting entities and prescribes certain measures for knowing your client. These measures align with privacy principles as the information that is required is for “knowing your client” purposes.

The Office of the Privacy Commissioner of Canada can provide further guidance, and has created a question and answer document about PIPEDA and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*,⁴¹⁶ to help clarify your responsibilities under PIPEDA.

⁴¹⁶ Office of the Privacy Commissioner of Canada, *PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, March 28, 2012

12.1 Summary of “know your client” requirements

Table 13

“Know your client” requirements	Not required for “know your client”
<ul style="list-style-type: none">• identification information (type of identification document, identification reference number, place of issue)• occupation information• date of birth• address	<ul style="list-style-type: none">• copy of the identification document• the inclusion of your client’s Social Insurance Number in a report to FINTRAC

12.2 Where AML/ATF and privacy get complicated

The AML/ATF legislation requires that reporting entities apply a risk-based approach. This means that resources are allocated to areas of high risk in order to mitigate the risks. Based on the risk assessment that is required to be conducted and documented by all reporting entities, clients that have been identified as a high risk for money laundering or a terrorist financing offence should be subjected to enhanced measures. The AML/ATF legislation provides some indication of what enhanced measures⁴¹⁷ are but they are not prescriptive. Section 6.3.6 provides some examples of enhanced measures but it may be important to consult an expert to ensure they do not conflict with privacy legislation.

12.3 What does the AML/ATF legislation say about enhanced measures?

The AML/ATF legislation requires prescribed special measures to be applied and enhanced measures taken. The AML/ATF legislation also states that “any other enhanced measures” are to be applied to mitigate the risks. This allows reporting entities to apply their own controls, on top of the prescribed special or enhanced measures.

417 PCMLTFR section 157

12.4 What is required for enhanced measures?

When applying “other enhanced measures” for high-risk clients, it is important that these measures be defined in the compliance policies and procedures and that these measures are clearly articulated with documented reasoning for collecting additional information.

12.5 What information should be documented?

The information that should be documented includes:

1. rationale – For collecting information that is in addition to the standard request
2. process – What information is to be collected for prescribed special measures, when enhanced measures are to be applied, and when and how information is to be collected

Important Notes: Remember that it is acceptable to let the client know that the information that you are asking for is required under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, unless disclosing this would tip off the client about a completed or attempted suspicious transaction report.

CHAPTER 13

Interactions with other reporting entities

There are several things to keep in mind when you are dealing with other reporting entities. All reporting entities, as defined in the AML/ATF legislation, have specific AML/ATF obligations that are unique to their type of entity, as with accountants and accounting firms.

In the course of your interactions with other financial entities, when you are conducting services on behalf of your clients, you may be called upon to provide other information based on the activities of your clients.

Be aware that AML/ATF obligations require that reporting entities are adequately identifying their clients, understanding their clients' activities and are applying a risk-based approach to their clients' activities. Information that may be requested will have to do with complying with these obligations.

You should also be aware that you may need to interact with other reporting entities when identifying a person or an entity. The AML/ATF legislation allows you to use the reliance method (See Chapters 23 and 24 of this guide) to do so. To use that method means relying on another reporting entity (RE) to verify the identity of the person or entity on your behalf where certain requirements will need to be met such as obtaining the person's name; having a written agreement or arrangement with the other RE for the purpose of verifying a person's identity; and obtaining all the information that the other RE referred to in order to verify the identity of the person.

CHAPTER 14

Sanctions

The AML/ATF legislation identifies two sets of sanctions that may be applied to reporting entities: administrative monetary penalties (AMPs) and criminal-type offences. FINTRAC has the legislative authority to apply AMPs against the entity and a person where significant non-compliance has been identified. FINTRAC does not conduct criminal-type investigations and does not pursue to charge, with the Public Prosecution Service of Canada's approval, a person or an entity with an offence under the AML/ATF legislation. FINTRAC is not an investigative body. FINTRAC may also disclose and refer cases of non-compliance to law enforcement to pursue criminal charges when it believes that the seriousness of the non-compliance would be relevant to an investigation into an offence of the AML/ATF legislation.

The PCMLTFA is clear that a violation is not an offence.⁴¹⁸ The choice that FINTRAC makes when pursuing sanctions is 1) either it imposes an administrative monetary penalty or 2) it refers the case to the police to investigate and pursue criminal charges. A person or an entity cannot be imposed both an administrative monetary penalty and be convicted of an offence under the PCMLTFA and its regulations.

14.1 Administrative monetary penalties (AMPs)

FINTRAC may issue an AMP⁴¹⁹ and serve a notice of violation when it has reasonable grounds to believe that a reporting entity has violated a requirement of the AML/ATF legislation. The amount of penalty imposed is determined taking into account:

- that administrative monetary penalties are meant to encourage compliance rather than punish⁴²⁰

⁴¹⁸ PCMLTFA subsection 73.23(1) "For greater certainty, a violation is not an offence"

⁴¹⁹ FINTRAC, *Administrative monetary penalties policy*, August 29, 2019

⁴²⁰ PCMLTFA subsection 73.11

- the harm done by the violation
- the history of compliance by the person or entity with the AML/ATF legislation
- any other criteria that may be prescribed by regulation

The process that FINTRAC follows before imposing a monetary penalty is two-fold.

1. FINTRAC assesses the non-compliance
 - severity of the non-compliance understanding the extent and the root cause of the non-compliance
 - impact on FINTRAC’s intelligence mandate and on the achievement of the objectives of the Act
 - other factors such as the reporting entity’s compliance history with the AML/ATF legislation
2. FINTRAC decides how to address the non-compliance

Following the completion of a compliance assessment, and depending on the extent of the non-compliance identified, FINTRAC may decide to:

 - take no further action
 - conduct follow-up compliance activities
 - issue an AMP to encourage a change in behaviour, or
 - disclose relevant information to law enforcement for investigation and prosecution of non-compliance offences under the AML/ATF legislation

FINTRAC has indicated that AMPs are not issued automatically in response to non-compliance. AMPs are one tool that is available to FINTRAC and are used to address repeated non-compliant behaviour. AMPs may also be used when there are significant issues of non-compliance or a high impact on FINTRAC’s intelligence mandate or on the objectives of the AML/ATF legislation. An AMP is generally used when other compliance options have failed.

14.1.1 Categories of violations

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) list the non-compliance violations that could be the basis of an AMP. The AMP Regulations categorize violations by degree of importance, and assign the following penalty ranges:

Table 14⁴²¹

Categories of violations	
Minor violation	\$1 to \$1,000 per violation
Serious violation	\$1 to \$100,000 per violation
Very serious violation	\$1 to \$500,000 per violation ⁴²²

The limits above apply to each violation, and multiple violations can result in a total amount that exceeds these limits.

14.1.2 AMP process

The AMP process begins with the issuance of a notice of violation and continues as outlined below:

- notice of violation:
 - FINTRAC must issue a notice of violation no more than two years from the date when the non-compliance became known to FINTRAC.
 - In some cases, FINTRAC may exercise its discretion to offer to enter into a compliance agreement with the reporting entity, which will include specific terms and conditions.
 - The notice provides information on the right to make written representations to FINTRAC’s director and chief executive officer (CEO), up to 30 days after receiving the notice of violation.
- payment of penalty:
 - Upon receipt of a notice of violation, a person or entity can pay the penalty by completing the remittance form and submitting it with the payment in Canadian funds to FINTRAC.
 - If a reporting entity pays the penalty indicated in the notice of violation, the reporting entity is deemed to have committed the violations specified, and the AMP process ends.
- representations to FINTRAC’s director and CEO:
 - A reporting entity may request a review of a notice of violation. This can be done by making written representations on the violations or the penalty or both at the same time, to the director and CEO of FINTRAC, within 30 days of receiving the notice of violation.
 - If a reporting entity requests a review, FINTRAC’s director and CEO will decide whether there is proof on a balance of probabilities that the reporting entity committed the violation or not; and may impose

⁴²¹ PCMLTFAMPR section 5

⁴²² Please note that FINTRAC’s AMP policy <https://www.fintrac-canafe.gc.ca/pen/2-eng> states that the penalty amount for a very serious violation is as follows: \$1 to \$100,000 per violation for an individual and \$1 to \$500,000 per violation for an entity.

the penalty proposed in the notice of violation, a lesser penalty or no penalty. The director and CEO will issue notice of decision to communicate the decision and the rationale for it.

- failure to pay or make representations and notice of penalty:
 - If a reporting entity receives a notice of violation and does not pay or make representations to FINTRAC's director and CEO within 30 days, the reporting entity will be deemed to have committed the violation, and FINTRAC will impose the penalty in respect of it.
- notice of decision and right of appeal:
 - A reporting entity that receives a notice of decision from FINTRAC's director and CEO has 30 days to exercise its right of appeal to the Federal Court of Canada. The AMP process ends when a reporting entity pays the penalty imposed in the notice of decision or does not appeal the director and CEO's decision within 30 days.
 - Should the director and CEO not issue a notice of decision within 90 days of receiving the representation for review, a person or entity may appeal the proposed penalty to the Federal Court within 30 days.
- Federal Courts:
 - The Federal Courts have the power to confirm, set aside or change a notice of decision issued by FINTRAC's Director and CEO. As long as the AMP is before the Federal Court, the Federal Court of Appeal, or the Supreme Court of Canada, the AMP process is considered to be ongoing.
- public notice:
 - FINTRAC must make public, as soon as feasible, the name of the reporting entity, the nature of the violation or default, and the amount of the penalty imposed in the following cases:
 - » a reporting entity pays the penalty issued in a notice of violation
 - » a reporting entity neither pays the penalty issued in a notice of violation nor makes representations to FINTRAC's director and CEO
 - » a reporting entity receives a notice of decision indicating that a violation has been committed
 - » a reporting entity enters into a compliance agreement with FINTRAC
 - » a reporting entity does not comply with a compliance agreement

- AMPs imposed by FINTRAC are published on the public notice page.⁴²³
- collection of penalties:
 - The penalty amount is due 30 days after the notice of violation or notice of decision is received by the reporting entity. Interest begins to accrue on the day after the penalty was due. Any penalty that becomes payable is an outstanding debt to the Crown. FINTRAC will pursue outstanding AMP payments.

14.2 Voluntary self-declaration of non-compliance

FINTRAC has a policy of relief when a reporting entity comes forward to self-disclose non-compliance with the AML/ATF legislation. Its policy on voluntary self-declaration of non-compliance is explained on its website.⁴²⁴

FINTRAC encourages compliance with the AML/ATF legislation by recognizing that when reporting entities periodically review their program, conduct ongoing risk assessment or quality control activities, they may come across instances where they have not met all the requirements of the AML/ATF legislation. FINTRAC indicates these shortfalls may be in relation to reporting, client identification, record keeping or effectively implementing an area of the reporting entity's compliance program.

Unreported transactions still have intelligence value to FINTRAC and need to be reported, while other shortfalls need to be addressed without delay. The ultimate goal of the regulatory regime is to enhance compliance, not to impose penalties.⁴²⁵ Therefore, FINTRAC has implemented a policy to encourage reporting entities to voluntarily declare their non-compliance in order to resolve the issues they identify. The information that must be included in a voluntary self-declaration of non-compliance must be made in writing. The information required is specified on FINTRAC's website⁴²⁶ as is the form.⁴²⁷

FINTRAC advises that when the voluntarily declared non-compliance issue is not a repeated instance of a previously voluntarily disclosed issue, and when this declaration has not been made after a reporting entity has been notified of an upcoming examination, FINTRAC will work with the reporting entity to resolve

423 FINTRAC, *Public notice of administrative monetary penalties*, December 10, 2021

424 FINTRAC, *Voluntary Self-Declaration of Non-Compliance*, November 20, 2020

425 Ibid

426 Ibid

427 FINTRAC, *Voluntary self-declaration of non-compliance form*, June 1, 2021

the issue and will not propose enforcement actions, such as an administrative monetary penalty related to the submission. Voluntary self-declarations of non-compliance should be sent to: VSDONC.ADVNC@fintrac-canafe.gc.ca⁴²⁸

14.2.1 What FINTRAC's assessment manual indicates on voluntary self-declarations of non-compliance⁴²⁹

If an accountant or accounting firm identifies non-compliance after **a FINTRAC examination** has started, they should inform the FINTRAC officer immediately and send a voluntary self-declaration of non-compliance to FINTRAC. FINTRAC considers the date on which it notified the accountant or accounting firm of the examination to be the start of the examination (e.g., notification call).

When FINTRAC receives a voluntary self-declaration of non-compliance on an issue that was not previously voluntarily disclosed **before a FINTRAC examination has started**, it will not consider enforcement actions, such as an administrative monetary penalty.

However, if FINTRAC receives a self-declaration **during an examination**, it will assess the non-compliance as part of the examination, work with the reporting entity to correct it, and determine if the non-compliance warrants an enforcement action. For example, if the accountant or accounting firm did not submit a financial transaction report to FINTRAC when required and then submits it after the notification date, FINTRAC will consider that the accountant or accounting firm did not meet its requirement to submit the report. In addition, there may be situations where compliance program documents (for example, compliance policies and procedures) are created or adjusted after the notification date. In such cases, FINTRAC may determine that the accountant or accounting firm did not meet the compliance program requirements.

14.3 Offences⁴³⁰

The PCMLTFA identifies criminal-type offences for non-compliance for persons or entities that knowingly contravene the prescribed sections of the AML/ATF legislation. For general offences and offences related to contravention to a directive, the offences call for:

428 FINTRAC, *Voluntary self-declaration of non-compliance*, November 20, 2020

429 FINTRAC, *Assessment Manual*, March 21, 2022

430 PCMLTFA Part 5 Offences and Punishment

- a. on summary conviction, to a fine of not more than \$250,000 or to imprisonment for a term of not more than two years less a day, or to both, or
- b. on conviction on indictment, to a fine of not more than \$500,000 or to imprisonment for a term of not more than five years, or to both

For offences related to reporting and regulations (1) Every person or entity that knowingly contravenes section 7 or 7.1, or (2) any regulation made under subsection 11.49(1) is guilty of an offence and liable:

- a. on summary conviction, to a fine of not more than \$1,000,000 or to imprisonment for a term of not more than two years less a day, or to both, or
- b. on conviction on indictment, to a fine of not more than \$2,000,000 or to imprisonment for a term of not more than five years, or to both

CHAPTER 15

Appendix A - Summary table of requirements when dealing with business relationships and a PEFP, PEDP, HIO, their family members or close associates

Note: When referring to **both** a politically exposed foreign person and a politically exposed domestic person, this guide, like FINTRAC's guidance, may use the term PEP (politically exposed person).

The AML/ATF legislation has identified specific requirements in dealing with a politically exposed foreign person, a politically exposed domestic person, a head of an international organization, a family member and close associate.

FINTRAC's guidance documents⁴³¹ outline requirements for accountants and accounting firms as a **non-account-based reporting entity sector**. You must take reasonable measures to make a business relationship related PEP, HIO, family member or close associate (of foreign PEP only, in certain circumstances) determination when you:

1. **Enter into a business relationship** (i.e., the second time you verify the identity of the person) with a politically exposed foreign person, a politically exposed domestic person, a head of an international organization, a family member of one of those persons or a person

⁴³¹ FINTRAC, *Politically exposed persons and heads of international organizations guidance for non-account-based reporting entity sectors*, June 11, 2021, FINTRAC *Politically exposed persons and heads of international organizations guidance*, May 4, 2021 and FINTRAC, *Frequently asked questions about domestic politically exposed persons and heads of international organizations*, June 1, 2021.

who is closely associated with a politically exposed foreign person. In such a case you must take reasonable measures to determine whether a person with whom you enter into a business relationship is a PEP, HIO, family member of one of those persons or a close associate of a politically exposed foreign person.⁴³²

2. **Conduct periodic monitoring of your business relationships.** In this situation, you must take reasonable measures to determine whether the person with whom you have a business relationship is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization, a family member of one of those persons or a person who is closely associated with a politically exposed foreign person.
3. **Detect a fact about your existing business relationships that indicates a PEP or HIO connection.** If you or any of your employees or officers detect a fact that constitutes reasonable grounds to **suspect that a person with whom you have a business relationship** is a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.

When you **enter into a business relationship** with, or **detect a fact** about a PEP, HIO, or family member or close associate of one of these persons, you have **30 days** after the day on which you enter into the business relationship or detect a fact, to take reasonable measures to establish the source of a person's wealth, if applicable.⁴³³

Based on FINTRAC's guidance,⁴³⁴ the following Table 15 describes for each of foreign PEPs, domestic PEPs or a HIO, or a family member or close associate of one of these persons, the length of time considered to be one those persons.

432 PCMLTFR subsection 120.1(1)

433 PCMLTFR subsection 122.1(5)

434 PCMLTFR subsection 2(2) and FINTRAC "Politically exposed persons and heads of international organizations guidance", May 4, 2021 Also refers to Policy Interpretation PI-4606 (see Section 20.5 of this guide) and with the caution indicated about the applicability of each Policy Interpretation.

Table 15

Definition	Length of time considered to be one those persons
Politically exposed foreign person	Once it is determined that a person is a foreign PEP, they remain a foreign PEP forever , including deceased foreign PEPs. You are not required to determine whether they are a foreign politically exposed person again.
Family member of a foreign PEP	Once you determine that a person is a family member of a foreign PEP (including a deceased foreign PEP), they remain a family member of a foreign PEP forever and you are not required to make this determination again.
Politically exposed domestic person	A person ceases to be a domestic PEP five years after they have left office or five years after they are deceased Note: You must continue to mitigate the risks associated with domestic PEPs until they cease to be domestic PEPs.
Family member of a domestic PEP or HIO	A person ceases to be considered a family member of a domestic PEP or HIO five years after the domestic PEP or HIO has left office (including upon death). In the case of a deceased domestic PEP or HIO, persons that are their family members remain a family member of a domestic PEP or HIO for five years after the domestic PEP or HIO ceases to be a domestic PEP or HIO. Note: you must continue to mitigate the risks associated with the family members of domestic PEPs or HIOs during that time.
Head of international organization	A HIO, five years after they are no longer the head of the organization or institution or five years after they are deceased. Note: You must continue to mitigate the risks associated with HIOs until they cease to be HIOs.
Close associate of a PEP or HIO	Once you determine that a person is the close associate of a PEP or HIO, they remain a close associate until they lose that connection.

15.1 Definitions

Head of an international organization⁴³⁵ means a person who, at a given time, holds or has held within five years before that time the office or position of head of an international organization that is established by the governments of states or the head of an institution of any such organization.

Politically exposed domestic person⁴³⁶ means a person who, at a given time, holds or has held within a five-year period before that time, one of the offices or positions referred to in any of paragraphs (a) to (j) (see further) in or on behalf of the federal government or a provincial government or the office or position referred to in paragraph (k) in a municipal government: (a) Governor General, lieutenant governor or head of government; (b) member of the

435 PCMLTFA subsection 9.3 (3) and PCMLTFR subsection 2(2)
436 Ibid

Senate or House of Commons or member of a legislature; (c) deputy minister or equivalent rank; (d) ambassador, or attaché or counsellor of an ambassador; (e) military officer with a rank of general or above; (f) president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province; (g) head of a government agency; (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada; (i) leader or president of a political party represented in a legislature; (j) holder of any prescribed office or position; or (k) mayor.

Politically exposed foreign person⁴³⁷ means a person who holds or has held one of the following offices or positions in or on behalf of a foreign state: head of state or head of government; member of the executive council of government or member of a legislature; deputy minister or equivalent rank; ambassador, or attaché or counsellor of an ambassador; military officer with a rank of general or above; president of a state-owned company or a state-owned bank; head of a government agency; judge of a supreme court, constitutional court or other court of last resort; leader or president of a political party represented in a legislature; or holder of any prescribed office or position.

A **prescribed family member** of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is their spouse or common-law partner; their child; their mother or father; the mother or father of their spouse or common-law partner; or a child of their mother or father.⁴³⁸

In all of these cases there are additional reasonable measures and/or special measures and record keeping requirements to be met. Three tables summarizing these requirements are provided in Sections 15.2, 15.3 and 15.4.

437 PCMLTFA subsection 9.3(3)
438 PCMLTFR subsection 2(1)

15.2 Requirements when entering into a business relationship

Table 16A

Requirements when entering into a business relationship with a politically exposed foreign person (PEFP), or a family member of, or a person who is closely associated with a PEFP

Requirement	Records to keep	Regulatory references
<p>Once you enter into a business relationship and determine that a person is a politically exposed foreign person (PEFP), or a family member of, or a person who is closely associated with a politically exposed foreign person, you must:</p> <ol style="list-style-type: none"> a. take reasonable measures within 30 days after the day on which you enter into the business relationship with a PEFP, to establish the source of the person's wealth b. take enhanced measures⁴³⁹ such as: <ul style="list-style-type: none"> — additional measures to verify the identity of the person — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., suspicious transaction reports) — any other enhanced measures to mitigate the risks posed by the person 	<p>You must keep a record⁴⁴⁰ of:</p> <ol style="list-style-type: none"> a. the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed foreign person b. the date of the determination c. the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 120.1(1), 122.1(1), 122.1(6), 123(4), paragraph 148(1)(c), section 157</p>

⁴³⁹PCMLTFR Section 157: The prescribed special measures that are required to be taken by a person or entity referred to in subsection 9.6(1) of the Act for the purposes of subsection 9.6(3) of the Act are the development and application of written policies and procedures for (a) taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity; and (b) taking any other enhanced measure to mitigate the risks, including (i) ensuring, at a frequency appropriate to the level of risk, that client identification information and information collected under section 138 is up to date, and (ii) conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships referred to in section 123.1

⁴⁴⁰PCMLTFR subsection 123(4)

Table 16B

Requirements when entering into a business relationship with a politically exposed domestic person (PEDP), a head of an international organization (HIO) or a family member of a PEDP or HIO

Requirement	Records to keep	Regulatory references
<p>Once you enter into a business relationship and determine that a person is a politically exposed domestic person (PEDP), a head of an international organization (HIO) or a family member of a politically exposed domestic person or HIO, and you consider based on your risk assessment that there is a high risk of the person being involved in a money laundering or terrorist financing activity, you must</p> <ol style="list-style-type: none"> a. take reasonable measures within 30 days after the day on which you enter into the business relationship with a PEDP or HIO to establish the source of the person's wealth if applicable b. take enhanced measures such as: <ul style="list-style-type: none"> — taking additional measures to verify the identity of the person — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., suspicious transaction reports) — any other enhanced measures to mitigate the risks posed by the person 	<p>You must keep a record of:</p> <ol style="list-style-type: none"> a. the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed domestic person, or HIO b. the date of the determination c. the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 120.1(1), 122.1(3), 122.1(6), 123(4), paragraph 148(1)(c) and section 157</p>

15.3 Requirement to conduct periodic monitoring of your business relationships

Table 17A

Requirements to conduct periodic monitoring of your business relationship to determine if they are a PEFP, or a family member of, or a person who is closely associated with a PEFP

Requirement	Records to keep	Regulatory references
<p>Once you conduct periodic monitoring of a business relationship and you determine that a person is a politically exposed foreign person (PEFP), or a family member of, or a person who is closely associated with a politically exposed foreign person, you must:</p> <ul style="list-style-type: none"> a. take reasonable measures to establish within 30 days after the day on which you enter into the business relationship with a PEFP the source of the person's wealth b. take enhanced measures such as: <ul style="list-style-type: none"> — taking additional measures to verify the identity of the person — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., Suspicious Transaction Reports) — any other enhanced measures to mitigate the risks identified 	<p>You must keep a record⁴⁴¹ of:</p> <ul style="list-style-type: none"> a. the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed foreign person b. the date of the determination c. the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 120.1(2), 122.1(1), 123(4), and paragraph 148(1)(c), section 157</p>

441 PCMLTFR subsection 123(4)

Table 17B

Requirements to conduct periodic monitoring of your business relationships to determine if they are a PEDP, a HIO or a family member of one of those persons

Requirement	Records to keep	Regulatory references
<p>Once you conduct periodic monitoring of a business relationship and you determine that a person is a politically exposed domestic person, a head of an international organization or a family member of one of those persons, and you consider, based on your risk assessment⁴⁴² that there is a high risk of a money laundering offence or terrorist activity financing offence being committed, you must:⁴⁴³</p> <ul style="list-style-type: none"> a. take reasonable measures to establish within 30 days after the day on which you enter into the business relationship with a PEDP or HIO the source of the person's wealth b. take enhanced measures⁴⁴⁴ such as: <ul style="list-style-type: none"> — taking additional measures to verify the identity of persons and entities — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., suspicious transaction reports) — taking any other enhanced measures to mitigate the risks posed by the person 	<p>You must keep a record of:</p> <ul style="list-style-type: none"> a. the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed domestic person or a head of an international organization, or a family member of one of those persons b. the date of the determination c. the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 122.1(3), 122.1(6), 123(4), paragraph 148(1)(c), section 157</p>

442 PCMLTFA subsection 9.6(2)

443 PCMLTFR paragraphs 122.1(1)(a) and (b)

444 PCMLTFR section 157

15.4 Requirements when you detect a fact that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is a PEFP, a family member, or close associate of a PEFP

Table 18A

Requirements when you detect a fact that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is a PEFP, a family member, or close associate of a PEFP

Requirement	Records to keep	Regulatory references
<p>Once you or your employees detect a fact about an existing business relationship that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is a politically exposed foreign person, or a family member of, or a person who is closely associated with a politically exposed foreign person you must take reasonable measures to determine that they are such a person. If so, you must:</p> <ol style="list-style-type: none"> take reasonable measures within 30 days after the day on which the fact is detected, to establish the source of the person's wealth take enhanced measures⁴⁴⁵ such as: <ul style="list-style-type: none"> — additional measures to verify the identity of persons when they are assessed as high-risk clients — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., suspicious transaction reports); and — taking other enhanced measures to mitigate the risks posed by the person 	<p>You must keep a record of:</p> <ol style="list-style-type: none"> the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed foreign person, or a family member, or a person who is closely associated with that person the date of the determination the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 120(5), 120.1(4), 122.1(1), 122.1(6), 123(4), paragraph 148(1)(c), section 157</p>

⁴⁴⁵PCMLTFR Section 157: The prescribed special measures that are required to be taken by a person or entity referred to in subsection 9.6(1) of the Act for the purposes of subsection 9.6(3) of the Act are the development and application of written policies and procedures for (a) taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity; and (b) taking any other enhanced measure to mitigate the risks, including (i) ensuring, at a frequency appropriate to the level of risk, that client identification information and information collected under section 138 is up to date, and (ii) conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships referred to in section 123.1.

Table 18B

Requirements when you detect a fact that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is a PEDP, a HIO, or a family member of a PEDP or HIO

Requirement	Records to keep	Regulatory references
<p>Once you detect a fact that constitutes reasonable grounds to suspect that the person with whom you have a business relationship is a politically exposed domestic person, a head of an international organization or a family member of one of those persons, and you consider, based on your risk assessment, that there is a high risk of a money laundering offence or terrorist activity financing offence being committed, you must:</p> <ol style="list-style-type: none"> a. take reasonable measures to establish the source of the person's wealth b. take enhanced measures such as: <ul style="list-style-type: none"> — taking additional measures to verify the identity of persons when they are assessed as high-risk clients — conducting enhanced ongoing monitoring of the business relationship for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., Suspicious Transaction Reports) — taking other enhanced measures to mitigate the risks posed by the person <p>You must take reasonable measures to establish the source of the person's wealth within 30 days after the day on which the fact is detected, if applicable.</p>	<p>You must keep a record of:</p> <ol style="list-style-type: none"> a. the office or position and the name of the organization or institution in respect of which the person is determined to be a politically exposed domestic person or a head of an international organization, or a family member of, one of those persons b. the date of the determination c. the source, if known, of the person's wealth <p>Retention: You must keep these transaction records for at least five years after the day on which they were created.</p>	<p>PCMLTFR subsections 122.1(3), 123(4), 122.1(6) paragraph 148(1)(c), section 157</p>

CHAPTER 16

Appendix B – Canada’s AML/ATF regime

16.1 Players

There are a wide range of players that are part of Canada’s AML/ATF regime. They range from individuals to entities and from federal departments to international entities. Below is a summary of the players:

Table 19

Who has reporting requirements to FINTRAC?	<p>Reporting entities:</p> <ul style="list-style-type: none">• financial institutions• life insurance companies and life insurance brokers or agents• legal counsel and legal firms (not operative at present)• securities dealers• money service businesses• accountants and accounting firms• British Columbia notaries• real estate brokers, sales representatives, and real estate developers• dealers in precious metals and stones• casinos <p>Federal entity that has a requirement to provide cross-border currency reports, seizures and forfeitures to FINTRAC:</p> <ul style="list-style-type: none">• Canada Border Services Agency
---	--

<p>What is FINTRAC?</p>	<p>FINTRAC is Canada's financial intelligence unit. It has a dual function. It provides financial intelligence related to money laundering, terrorist financing and threats to the security of Canada to designated recipients (police, CRA, CBSA, CSIS, Agence du Revenu du Québec, Competition Bureau, Communications Security Establishment. etc.) and is responsible for the overall supervision of reporting entities to determine compliance with Canada's AML/ATF regime.</p> <p>FINTRAC is an independent agency whose legislation is the responsibility of the Department of Finance. FINTRAC is subject to review by the following departments:</p> <ul style="list-style-type: none"> • Office of the Privacy Commissioner of Canada • Office of the Auditor General of Canada
<p>Who does FINTRAC share information with?</p>	<p>FINTRAC may disclose information if it has reasonable grounds to suspect that the information would be relevant to an investigation or prosecution of a money laundering or terrorist activity financing offence, or relevant to threats to the security of Canada.</p> <p>Once FINTRAC reaches a threshold for disclosure it must disclose to police. The following is a list of agencies FINTRAC may disclose information to when certain conditions are met:</p> <ul style="list-style-type: none"> • Canadian Security Intelligence Service • Communications Security Establishment • CRA • Agence du revenu du Québec • Canada Border Services Agency • Foreign financial intelligence units • Competition Bureau • an agency or body that administers the securities legislation of a province • Department of National Defence and the Canadian Forces

16.2 FINTRAC's roles

FINTRAC is Canada's financial intelligence unit. It is an independent agency that was established to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* and its regulations. It has two key operational mandates⁴⁴⁶. First, it assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities by analysing and disclosing financial intelligence to police and designated recipients. Secondly, it has a supervisory responsibility for ensuring compliance of reporting entities with the legislation and regulations and maintaining a registry of money services businesses in Canada. It is with FINTRAC's compliance operations and function that accountants and accounting firms will be most familiar on an on-going basis.

⁴⁴⁶More on [FINTRAC's mandate](#).

FINTRAC publishes on its website a great deal of information to assist reporting entities. You will find in Chapter 17, Appendix C, links to relevant Guidance on a series of topics, Interpretation Notices, Policy Interpretations and other publications and services.

16.3 FINTRAC assistance

16.3.1 Guidance

As part of its supervisory role, FINTRAC's approach to ensuring compliance is to provide information to reporting entities to facilitate compliance. The guidance section on FINTRAC's website provides explanations of its compliance framework based on three pillars (assistance, assessment and enforcement) and on the requirements for the compliance program, know your client, transactions reporting and record keeping.

16.3.2 Interpretation notices

Of the seven interpretation notices⁴⁴⁷ issued by FINTRAC two are relevant to accountants and accounting firms:

- FINTRAC Interpretation Notice 2: Accountants – Giving Instructions Versus Providing Advice
- FINTRAC Interpretation Notice 7: Insolvency Practitioners Providing Trustee in Bankruptcy Services

This guide has integrated the information from these two interpretation notices, which are found in their original text in Chapter 18 – Appendix D, Chapter 19 – Appendix E.

16.3.3 Policy interpretations

Policy interpretations⁴⁴⁸ are published as questions and answers from various reporting entity sectors on different topics (see Chapter 20 where the most relevant to accountants and accounting firms are reproduced in their original text). All FINTRAC policy interpretations may be found on FINTRAC's website under the categories of: Beneficial Ownership, Business Relationship, Compliance Program, Correspondent banking, Enforcement, Money services business/Foreign money services business, Ongoing Monitoring, Politically Exposed Persons or Heads of an International Organization, Record Keeping,

⁴⁴⁷ Policy interpretations are located under the Guidance tab of [FINTRAC's homepage](#).
⁴⁴⁸ FINTRAC, *Interpretation notices*, August 20, 2021

Reporting, Third-party Determination, Verifying Identity and Other.⁴⁴⁹

Caution: Accountants and accounting firms should be prudent when reading these interpretations as they are issued at a particular time in response to a specific question from an industry sector. FINTRAC warns that:

“Each policy interpretation reflects the requirements of the PCMLTFA and associated regulations in force at the time they were written. Legislative and regulatory amendments may have taken place since the policy interpretation was issued that may impact the determination made at the time. Therefore, please take note of the date each policy interpretation request was answered.”

With changing AML/ATF legislation over time, there may be differences in interpretation from FINTRAC given the time lapse. To the extent possible, this guide makes references to policy interpretations that are expected to be used by FINTRAC over the long-term. However, FINTRAC’s caveat should be observed.

16.3.4 Other FINTRAC publications and services

FINTRAC has other publications on its site and has produced multimedia videos and presentations, strategic intelligence reports and operational briefs on certain subjects. It also offers help with technical matters when using its F2R reporting application, validation rules or other technical difficulties. Assistance with policy interpretations may also be addressed to FINTRAC using the “Contact Us” section on their website.⁴⁵⁰

Accountants and accounting firms should consider subscribing to FINTRAC’s mailing list⁴⁵¹ to ensure that your compliance program reflects the latest AML/ATF legislation updates and communications from FINTRAC. This is an important consideration since FINTRAC has indicated in its assessment manual⁴⁵² that when it conducts an examination on the “two-year effectiveness review,” it will “look at the scope of the review (what the review covered) and methodology (how the review was conducted) and... assess whether your policies and procedures, risk assessment and ongoing compliance training program have been reviewed and cover the **current legal requirements and your current operations...**”

449 FINTRAC, *Policy interpretation database*

450 FINTRAC, *Contact Us*, May 12, 2021

451 FINTRAC, *FINTRAC mailing list*, August 16, 2019

452 FINTRAC, *FINTRAC assessment manual*, March 21, 2022, and Section 16.4.2 of this guide.

16.4 FINTRAC examinations

The AML/ATF legislation allows FINTRAC to conduct examinations on reporting entities. The examination involves a review of records and inquiries into the business for the purpose of ensuring compliance with Parts 1 and 1.1 of the PCMLTFA and the relevant regulations.

16.4.1 FINTRAC's powers

FINTRAC examinations are legislated under section 62(1) of the PCMLTFA. It specifically states that “An authorized person may, from time to time, examine the records and inquire into the business and affairs of any person or entity referred to in section 5 for the purposes of ensuring compliance with Part 1 or 1.1...”

This power includes allowing an authorized person to enter any premises where there are records related to the business and access any computer system to examine any data and to reproduce those records. Authorized persons would be FINTRAC officers who have been authorized by the director to ensure compliance under the PCMLTFA. In section 62(2) of the PCMLTFA, it explicitly states that reasonable assistance shall be given to authorized persons (FINTRAC officers).

16.4.2 FINTRAC's assessment manual

FINTRAC has published an assessment manual⁴⁵³ that describes in detail how FINTRAC conducts its compliance examinations. It is recommended you refer to the FINTRAC assessment manual should you be selected for a compliance examination.

FINTRAC conducts risk-based examinations, concentrating on issues or sectors where it assesses your business may be vulnerable to money laundering or terrorist activity financing risks and where there is a greater risk of not meeting the legal requirements (risk of non-compliance). Using this approach reduces burden on businesses by minimizing disruptions and ensuring the effective and efficient use of resources. FINTRAC expects you to provide it with, or make available, all relevant facts and information so when conducting an examination, they can make decisions based on complete information.

453 FINTRAC, *Assessment Manual*, March 21, 2022

16.4.3 Examination phases

Examinations are conducted on weekdays, during FINTRAC's regular business hours (8 a.m. to 5 p.m.). If these hours do not suit your business, FINTRAC asks that you notify them, as they may be able to offer some flexibility.

The number of days FINTRAC will spend on your premises will depend on the type, nature, size, and complexity of your business. For example, the examination of an Accountant, a smaller or medium-sized firm may take less than a week, while the examination of a larger firm may take several weeks.

FINTRAC examinations are broken down into three phases: planning and scoping; examination and assessment; and developing the findings and finalizing the examination. The examinations may be of two types: a desk examination or an on-site examination at your place of business. FINTRAC will inform you of the examination's location in a notification call and in a notification letter.

Requested documents, client records and records of transactions must be sent to FINTRAC for a preliminary review. When FINTRAC conducts an examination from their office, they hold telephone interviews with your compliance officer, employees and agents (if applicable).

When FINTRAC conducts an examination at your place of business, it will typically hold in-person interviews at your main location and may visit or call your other locations, if applicable, to conduct its interviews.

Note: In January 2022, FINTRAC announced a withdrawal of temporary COVID-related support to reporting entities, as noted below.⁴⁵⁴ FINTRAC issued a notice indicating it was resuming desk examinations on July 27, 2020 and being flexible with the implementation of some measures by reporting entities due to the COVID-19 pandemic. On November 16, 2020, FINTRAC issued another notice, and updated it on January 22, 2021, stating that it will exercise flexibility in assessing and enforcing compliance with certain record keeping and reporting obligations related to the amended regulations on June 1, 2021.⁴⁵⁵ While these measures may be temporary until COVID-19 protocols are lifted across Canada, and some administrative forbearance is exercised, accountants and accounting firms should take note of FINTRAC's May 18, 2021⁴⁵⁶ notice that states that:

FINTRAC will exercise flexibility and reasonability when assessing REs'

⁴⁵⁴ FINTRAC *Withdrawal of temporary COVID-related support to reporting entities*, January 31, 2022

⁴⁵⁵ FINTRAC, *Notice on forthcoming regulatory amendments and flexibility*, December 2, 2021

⁴⁵⁶ FINTRAC, *Notice on the assessment of obligations coming into force on June 1, 2021*, December 16, 2021

compliance with the amended Regulations. Using its operational policy that focusses on the examination period, FINTRAC will begin assessing compliance with the amended Regulations on April 1, 2022.

From June 1, 2021, to March 31, 2022, FINTRAC will assess compliance with the regulatory requirements in effect prior to June 1, 2021. During this period, FINTRAC will also review REs' most up-to-date compliance program elements. As REs must update their compliance program to reflect new regulatory requirements, this approach will provide REs with feedback to help them meet the requirements of the amended Regulations.

FINTRAC will begin assessing compliance with the amended Regulations on April 1, 2022. However, FINTRAC may assess transactional information for a period prior to April 1, 2022, while exercising reasonability and taking into consideration the flexible measures that FINTRAC has previously communicated in the "Notice on forthcoming regulatory amendments and flexibility."⁴⁵⁷

16.4.4 How to prepare for an examination

FINTRAC examinations are to ensure that you are complying with the AML/ATF legislation. When you receive confirmation from FINTRAC that they will be conducting an examination, there are a few points to keep in mind. Before receiving the letter confirming the examination, it is suggested that all compliance documentation be assembled and a review of past FINTRAC interactions be completed. The logistics of the examination should be finalized to ensure all documentation is assembled as quickly as possible and that sufficient staff is available to answer any supervisory questions. A room should be set aside for FINTRAC staff if they are coming to the premises and a photocopier should be made available for their use. Here are some additional things to keep in mind if you are having a FINTRAC compliance examination:

- Be aware of the deadlines that are noted in the letter from FINTRAC.
- If uncertain of any process, do not hesitate to call the FINTRAC officer conducting the examination.
- If you are aware of any deficiencies in your compliance program, or AML/ATF operations, before or during an examination you should refer to FINTRAC's policy and procedures for a voluntary self-declaration of non-compliance (see Section 14.2 of this guide).

⁴⁵⁷ FINTRAC, *Notice on forthcoming regulatory amendments and flexibility*, December 2, 2021

- Provide all documents and transactions that are listed in the letter from FINTRAC.
- Answer all questions calmly and honestly. Have resources available on hand during the examination.

16.4.5 What to expect

To summarize, the following list provides a summary of the examination process that you can expect during the exam:

1. Notification of examination: You will receive a call from FINTRAC notifying that they will be conducting a compliance examination. The call may include questions regarding your triggering activities.
2. Information request: Following the call, FINTRAC will send a letter requesting specific information. **Important note:** You usually have 30 days (sometimes 45 days depending on the size of the firm) from the date of the letter to provide all the information to FINTRAC.
3. Date of examination: The letter will also indicate the date when they will be conducting the examination. This can be either via conference call (desk examination) or on-site.
4. Examination: During the examination, FINTRAC will be asking the accountant's or accounting firms' compliance officer specific questions. These questions can include the following about your organization:
 - general business information
 - compliance regime
 - AML/ATF policies and procedures
 - risk assessment
 - ongoing training program
 - effectiveness compliance review
 - receipt of funds transactions
 - client identification
 - business relationship
 - collection of beneficial ownership information
 - ongoing monitoring
 - reporting
5. Exit interview: At the end of the examination, FINTRAC, either in person or by telephone, will discuss their preliminary findings with you. The findings are presented as “deficiencies.” Each deficiency is a violation of a provision in the AML/ATF legislation. At this time, you may offer additional information to help clarify a deficiency. You and FINTRAC will agree on a timeline for you to provide this material. After review of this material, FINTRAC may maintain its original deficiency, modify it or withdraw it.

16.4.6 Follow up

After FINTRAC's examination, you should expect to receive a letter from FINTRAC summarizing all deficiencies found during the examination. The language of the letter will clearly communicate the expectations that FINTRAC has from you in addition to any further actions being considered by FINTRAC. An action plan should be developed and implemented internally to rectify all deficiencies in a timely manner. At a later date, FINTRAC may decide to conduct a follow-up examination to ensure that you have addressed the deficiencies and have implemented your action plan. Therefore, it is important that you follow your action plan and that you document what has been done to address those deficiencies.

The consequences of non-compliance vary from minor such as the issuance of a findings letter asking for continued cooperation, to the severe with the issuance of a monetary penalty and a public naming summarizing all areas of non-compliance. The penalty amounts can be quite severe, and it is not uncommon to see penalties in the six-figure range. When egregious non-compliance has been observed by FINTRAC, the findings letter will explicitly state that administrative monetary penalties (AMP) are being considered. Regardless of the decision, FINTRAC will send additional correspondence notifying your organization of their final decision. Should no AMP be pursued, the letter will state that fact explicitly. However, if FINTRAC decides to pursue an AMP based on its analysis, a notice of violation will be issued to your organization.

Note: For more information, Section 14.1.2 explains in greater detail the AMP process.

Summary of the AMP process

If a notice of violation is received, your organization has several options available. Paying the penalty would close the proceedings and result in an admission of all violations from the non-compliance. Another option is to appeal the penalty directly with FINTRAC's director by providing explanations or arguments for any or all violations cited. This involves a secondary review of all violations to determine if any of the reasons within the appeal are reasonable. However, the request for a review must be in writing and submitted within 30 days of receiving the notice of violation. If this appeal is unsuccessful, a second appeal can be made to the Federal Court. It is prudent to obtain legal advice and professional AML/ATF assistance to help manage responses and appeals. However, regardless of the appeal process,

by law FINTRAC must publish the name of the person or entity, the amount and the nature of the violation. This in itself can be a significant damaging reputational risk to avoid.

Important note: Always document your progress. Documentation is important when it comes to showing FINTRAC that you are complying with the AML/ATF legislation and that you have addressed those deficiencies as stated in your action plan letter to FINTRAC.

16.4.7 Compliance assessment report

All reporting entities, including accountants and accounting firms, may be asked by FINTRAC to complete a compliance assessment report (CAR).⁴⁵⁸

The CAR is essentially a questionnaire which attempts to obtain a high-level overview of your organization's operations and if applicable, current level of compliance. However, as of the date of this publication, FINTRAC last used the compliance assessment reports tool in 2019 and has indicated that the system has recently been modified to enhance the process and FINTRAC plans on utilising it in the near future.

The information and advice given to accountants and accounting firms in the previous 2014 CPA guide was that the first section of the questionnaire will ask questions related to your scale of operations including financial information. The next section will ask questions regarding triggering activities to determine whether your organization is subject to the AML/ATF legislation. If the response to the triggering activities questions is positive, the remainder of the questionnaire will be specific to your legislative obligations and whether a compliance program has been developed and implemented. Given that FINTRAC has indicated it will resume its use of the CAR in the future, it is important to answer these questions truthfully as FINTRAC relies on this to populate their understanding of your organization and may contact your organization in the future to verify any information. If any part of the CAR is not fully understood, it is recommended that your organization contact FINTRAC for clarification.

⁴⁵⁸ Government of Canada, *Compliance assessment report*

CHAPTER 17

Appendix C – Links to FINTRAC guidance

Compliance program

Compliance program requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and associated regulations

<https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/Guide4/4-eng>

Risk assessment guidance

Risk-based approach

<https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng>

Know your client requirements

When to verify the identity of persons and entities – Accountants

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/client/acc-eng>

Methods to verify the identity of persons and entities

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng>

Business relationship requirements

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/brr-eng>

Ongoing monitoring requirements

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/omr-eng>

Beneficial ownership requirements

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/bor-eng>

Third party determination requirements

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/tpdr-eng>

Politically exposed persons, heads of international organizations, their family members and close associates

Politically exposed persons and heads of international organizations guidance

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/pep/pep-eng>

Politically exposed persons and heads of international organizations guidance for account-based reporting entity sectors

<https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/pep/pep-acct-eng>

Frequently asked questions about domestic politically exposed persons and heads of international organizations

<https://www.fintrac-canafe.gc.ca/publications/general/faq-pep-eng>

Transaction reporting requirements

What is a suspicious transaction report?

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng>

Reporting suspicious transactions to FINTRAC

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng>

Money laundering and terrorist financing indicators - Accountants

https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/accts_mltf-eng

Reporting terrorist property to FINTRAC

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng>

Large cash transactions

Guideline 7A: Submitting large cash transaction reports to FINTRAC electronically

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide7A/lctr-eng>

Guideline 7B: Submitting large cash transaction reports to FINTRAC by paper

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide7B/7b-eng>

Large virtual currency transactions

Reporting large virtual currency transactions to FINTRAC

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng>

Field instructions to complete a LVCTR

<https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng#annex1>

Large virtual currency transaction report form

<https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng>

Large virtual currency transaction reporting through the LVCTR Upload

<https://www.fintrac-canafe.gc.ca/reporting-declaration/info/lvctr-upload-eng>

Record keeping

Record keeping requirements for accountants

<https://www.fintrac-canafe.gc.ca/guidance-directives/recordkeeping-document/record/acc-eng>

Examinations

FINTRAC examinations: Your responsibilities and what you can expect from FINTRAC

<https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/05-2005/4-eng>

FINTRAC assessment manual

<https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/cam/cams-eng>

Voluntary self-declaration of non-compliance

<https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/vsdonc/1-eng>

Providing voluntary information about suspicions of money laundering or of the financing of terrorist activities

<https://www15.fintrac-canafe.gc.ca/vir-drtv/public/>

CHAPTER 18

Appendix D - FINTRAC Interpretation Notice No. 2

The following is a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

Source: <https://fintrac-canafe.canada.ca/guidance-directives/overview-apercu/fins/1-eng>

[**Note:** The definition of accountant has changed and now means a Chartered Accountant, a Certified General Accountant, a Certified Management Accountant or, if applicable, a Chartered Professional Accountant. Furthermore, the *CICA Handbook* is now referred to as the *CPA Canada Handbook*.]

FINTRAC Interpretation Notice No. 2

July 8, 2008

Accountants - Giving Instructions Versus Providing Advice

The purpose of this notice is to clarify the difference between providing advice to a client as opposed to giving instructions on behalf of a client, within the context of accountants' activities.

Accountants' activities

If you are an Accountant or an Accounting Firm, you are subject to certain requirements under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its regulations. This applies only when you engage in any of the following activities on behalf of any individual or entity (other than your employer), or give instructions in respect of those activities on behalf of any individual or entity (other than your employer):

- receiving or paying funds (for example you receive funds in trust to pay bills on behalf of your client);
- purchasing or selling securities, real estate property, business assets or entities; or
- transferring funds or securities by any means.

You are subject to the requirements when you engage in those activities, regardless of whether or not you receive any fees or have a formal letter of engagement to do so. In other words, even if you carry out these activities on a volunteer basis, you are subject to the PCMLTFA's requirements. Effective June 23, 2008, the receipt of professional fees themselves for the above mentioned activities does not trigger your requirements under the PCMLTFA.

Note: Activities of Accountants or Accounting Firms other than those listed above, such as audit, review or compilation engagements carried out according to the recommendations in the Canadian Institute of Chartered Accountants (CICA) Handbook, are not subject to the PCMLTFA or its regulations.

Giving instructions versus providing advice

When you give instructions for any of the above mentioned activities, it means that you actually direct the movement of funds. By contrast, when you provide advice to your clients, it means that you make recommendations or suggestions to them. Providing advice is not considered to be giving instructions.

Example of giving instructions: “Based on my client’s instructions, I request that you transfer \$15,000 from my client’s account, account number XXX, to account number YYY at Bank X in Country Z.”

Example of providing advice: “For tax purposes, we recommend that you transfer your money into a certain investment vehicle.”

For more information about the requirements applicable to Accountants and Accounting Firms, see the Guidance prepared by FINTRAC.

Date Modified: 2019-08-16

CHAPTER 19

Appendix E – FINTRAC Interpretation Notice No. 7

The following is a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

Source: <https://fintrac-canafe.canada.ca/guidance-directives/overview-apercu/fins/1-eng>

[**Note:** The definition of accountant has changed and now means a Chartered Accountant, a Certified General Accountant, a Certified Management Accountant or, if applicable, a Chartered Professional Accountant. Furthermore, the *CICA Handbook* is now referred to as the *CPA Canada Handbook*.]

FINTRAC Interpretation Notice no. 7

February 17, 2011

Insolvency Practitioners Providing Trustee in Bankruptcy Services

Paragraph 5(j) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and subsections 34(1), sections 35 and 36 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*.

The purpose of this notice is to clarify the application of the PCMLTFA relating to insolvency practitioners offering bankruptcy services.

Insolvency practitioners provide trustee in bankruptcy services. These services are not triggering activities for any obligations under the PCMLTFA. Trustee in bankruptcy services or insolvency practitioners are not covered as services or as an entity under our legislation. However, if you are an insolvency practitioner and you are an Accountant or an Accounting Firm, you may have obligations relating to other activities.

Insolvency practitioners who are accountants

If you are an individual Accountant or an Accounting Firm offering trustee in bankruptcy services or acting as an insolvency practitioner, you may have obligations under the PCMLTFA if you engage in certain triggering activities other than bankruptcy services. However, as explained above, bankruptcy services you provide as an insolvency practitioner, including acting as a trustee in bankruptcy, do not fall within the triggering activities under our legislation.

Definition of accountants

An accountant means a chartered accountant, a certified general accountant or a certified management accountant. An Accounting Firm means an entity that provides accounting services to the public that has at least one partner, employee or administrator that is an accountant.

In this context, if you are an insolvency practitioner, whether a chartered insolvency and restructuring professional or otherwise, you would not be considered to be “providing accounting services to the public” if you only provide such services as follows:

- As receiver, pursuant to the provisions of a Court order or by-way of a private letter appointment pursuant to the terms of a security interest
- As trustee in bankruptcy
- As monitor under the provisions of the *Companies’ Creditors Arrangement Act* or any other proceeding that results in the dissolution or restructuring of an enterprise or individual and to which the firm, individual or insolvency practitioner serves as an officer of the Court or agent to a creditor(s) or the debtor.

Triggering activities for accountants

If you are an Accountant or an Accounting Firm, as explained above, you have obligations under the PCMLTFA if you engage in any of the following activities on behalf of any individual or entity (other than your employer) or give instructions in respect of those activities on behalf of any individual 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.

In this context, an Accountant or an Accounting Firm appointed by a Court, or acting as a trustee in bankruptcy, is not considered to be acting on behalf of any other individual or entity.

Obligations under the PCMLTFA, as referred to throughout this interpretation notice, include reporting, client identification, record keeping, and implementing a Compliance Program. For more information about these, see FINTRAC's guidelines.⁴⁵⁹

Date Modified: 2019-08-16

⁴⁵⁹ FINTRAC, *Accountants*, July 12, 2021 (high-level summary of obligations for accountants)

CHAPTER 20

Appendix F – Relevant FINTRAC policy interpretations

This chapter includes a number of reproductions from the official content found on FINTRAC’s website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

Policy interpretations issued by FINTRAC provide useful guidance in determining how certain obligations may apply or when the language of the AML/ATF legislation appears unclear. However, while every attempt has been made to ensure that the FINTRAC policy interpretations remain applicable at the time of writing of this guide, the reader should bear in mind that references to the specific sections of the PCMLTFA or associated regulations may have changed from the time the policy interpretation was answered due to renumbering of the sections with each subsequent regulatory amendment. Many of the Policy Interpretations included here have now been archived on FINTRAC’s website with the following notice “This content is archived and will be kept online until March 31, 2022, for reference purposes only.”

This chapter includes a number of reproductions from the official content found on FINTRAC’s website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

20.1 Policy Interpretation PI No. 6171 answered on 2014-07-02: Clarification on record keeping retention⁴⁶⁰

Clarification on record keeping retention

⁴⁶⁰FINTRAC, *Archived Policy Interpretations - Record Keeping*, August 20, 2021

Question:

How long is an investment institution required to keep records of financial transactions that have been undertaken on behalf of their clients? What happens when the institution changes ownership or name ABC is now DEF?

Can a client recover the information through an InforSource Privacy Act request? How far back? What about if a person is attempting to acquire the information on behalf of an elderly parent who has signed a consent for the institution to release the information?

If a representative of an elderly person believes that a financial institution might be short selling investments just to acquire a commission what recourse is available to protect the elderly?

Answer:

FINTRAC administers the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations, so we can only address record retention requirements that are outlined in the legislation. That said, Canadian financial institutions have an obligation to collect and retain certain specific records relating to financial transactions and activities. The timeframes for keeping records depends on the nature of those records, and are as follows:

- In the case of signature cards, account operating agreements, client credit files, credit card applications, records setting out the intended use of the account, politically exposed foreign person records regarding an account, or a credit card account, these records have to be kept for five years from the day of closing of the account to which they relate.
- In the case of records to confirm the existence of an entity (including a corporation), beneficial ownership records, politically exposed foreign person records regarding transactions and records about a corresponding banking relationship, they have to be kept for five years from the day the last business transaction was conducted.
- In the case of a copy of a suspicious transaction report, the record has to be kept for a period of at least five years following the date the report was made.
- In the case of all other records, the records must be kept for a period of at least five years following the date they were created.

In some cases, reporting entities that acquire another entity will rely on the information collected by the acquired entity, and will consequently retain those records as if they had created them.

Date answered: 2014-07-02

PI Number: PI-6171

Obligation(s): Record Keeping

Guidance:

Regulations: 69(1)

20.2 Policy Interpretation PI No. 6303 answered on 2015-04-28: On accounting sector questions⁴⁶¹

Accountant Sector Questions

Question 1: Please define “Accounting Services”, and the concept of “to the public”, and explain the rationale and basis for those positions.

Question 2: Which of the following activities does FINTRAC consider to constitute “Accounting Services”:

- i. Assurance services
- ii. Specified auditing procedures
- iii. Compilation engagements
- iv. Forensic accounting
- v. Financial investigation
- vi. Financial litigation support services
- vii. Tax advisory services
- viii. Tax return preparation
- ix. Bookkeeping
- x. Trust administration
- xi. Escrow services
- xii. Corporate finance
- xiii. Clerical administration
- xiv. Chief Financial Officer services
- xv. Chief Operating Officer services
- xvi. Payroll administration
- xvii. Bank reconciliation services

⁴⁶¹ FINTRAC, *Archived Policy Interpretations - Other*, August 20, 2021

Question 3: Our question relates to various scenarios where accountants might be considered to be engaged in, or to be giving instructions on behalf of any person or entity, in respect of the following activities (“Triggering Activities”):

- i. receiving funds;
- ii. paying funds; and

Neither “Receiving”, nor “Paying” are defined terms in the PCMLTFA.

There are various scenarios which might be considered Triggering Activities, and would like your clarity in that regard.

Receiving Funds:

1. Would an Accountant be considered to have “received funds” if:
 - a. In the case of funds in the form cash or negotiable instruments, the Accountant physically collects the funds from the client’s safety deposit box on behalf of their client;
 - b. In the case of funds in the form cash or negotiable instruments, the Accountant physically gets funds from the client’s customer on behalf of their client;
 - c. In the case of funds in the form cash or negotiable instruments, the Accountant receives a deposit into their bank account from the client’s customer on behalf of their client;
 - d. In the case of funds in the form cash or negotiable instruments, the client receives a deposit into their account from a customer, an account which is monitored by their Accountant;
 - e. In the case of electronic funds (such as an EFT), the Accountant receives a deposit into their bank account from the client’s customer on behalf of their client; and,
 - f. In the case of electronic funds (such as an EFT), the client receives a deposit into their account from a customer, an account which is monitored by their Accountant.

Paying Funds:

2. Would an Accountant be considered to have been “paying funds” on behalf of their client, if:
 - a. If an Accountant pays for services on behalf of the client, using the Accountant’s cash;
 - b. If an Accountant pays for services on behalf of the client, using the client’s cash;
 - c. If an Accountant pays for services on behalf of the client, by mailing a cheque drawn on the Accountant’s account to the payee;

- d. If an Accountant pays for services on behalf of the client, by preparing a cheque drawn on the client's account, but signed by the client, and mailed by the Accountant to the payee;
- e. If an Accountant pays for services on behalf of the client, by preparing a cheque drawn on the client's account, but signed by the Accountant as an authorized signatory, and mailed by the Accountant to the payee;
- f. If an Accountant pays for services on behalf of the client, by preparing a cheque drawn on the client's account, but signed by the Accountant as an authorized signatory, and mailed by the client to the payee;
- g. If an Accountant pays for services on behalf of the client, by preparing a wire transfer drawn on the client's account, using internet banking privileges, but which is authorized for release by the client;

Question 4: What distinguishes a transfer on behalf of a client in the case of an Accountant, and a client remittance in the case of an MSB? Is it conceivable that a single entity could be considered to be at once an Accountant conducting a transfer on behalf of a client and an MSB remitting/transmitting funds at a client's instruction? If so, is it to the reporting entity to choose on which basis they will comply (Accountant or MSB)

Question 5: When all triggering activities are performed on behalf of an employer, an Accountant is exempted from the PCMLTFA requirements. While a Chief Financial Officer (CFO) would normally be an employee (with an employment contract), it is conceivable and common that a Chief Financial Officer (CFO) who is an Accountant is hired as a subcontractor, or indeed, that an Accounting Firm is contracted to perform the functions of a CFO, and that in the course of their duties, they conduct triggering activities. The CFO who is technically an employee clearly benefits from the exemption, and yet it is not clear that the contract-CFO enjoys that same exemption, despite the similarity in role and function. Could you please confirm that both contract CFOs who are Accountants, and contract CFOs who are Accounting Firms, enjoy the same exemption as their employee counterparts. Also, please confirm whether contract CFO services would be considered to be accounting services offered to the public.

Answer:

1. The terms “accounting services” and “to the public” are not defined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) or the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR).
2. Subsection 34(1) of the PCMLTFR states “subject to subsections (2) and (3), every accountant and every accounting firm is subject to Part 1 of the Act when they
 - a. engage in any of the following activities on behalf of any person or entity, namely,
 - i. receiving or paying funds,
 - ii. purchasing or selling securities, real properties or business assets or entities, or
 - iii. transferring funds or securities by any means; or
 - b. give instructions on behalf of any person or entity in respect of any activity referred to in paragraph (a).”

Therefore, it is only when an accountant or accounting firm engages in one of these activities that it becomes subject to Part 1 of the Act. If the listed services include the activities identified at subsection 34(1) of the PCMLTFR, then the accountant or accounting firm has obligations it must fulfil.

3. It will always be a question of fact to determine whether an activity falls under subsection 34(1) of the PCMLTFR, and specifically what it may be categorized as (i.e., receiving/paying funds or giving instructions).

3.1 (a - f): Most of the scenarios identified, with the exception of merely monitoring a client’s account, would likely fall under the activities described at subsection 34(1) of the PCMLTFR. That is, most of the scenarios may constitute receiving funds on behalf of a client or giving instructions for the receipt of funds on behalf of a client. Therefore, the accountant or accounting firm engaging in these activities, excluding solely monitoring a client’s account, would likely be subject to the PCMLTFA and its associated Regulations.

3. 2 (a - f): These scenarios would likely fall under the activities described at subsection 34(1) of the PCMLTFR. That is, each scenario may constitute paying funds on behalf of a client or giving instructions for the payment

of funds on behalf of a client. Therefore, the accountant or accounting firm engaging in these activities would likely be subject to the PCMLTFA and its associated Regulations.

4. The PCMLTFR defines an accountant as “a chartered accountant, a certified general accountant or a certified management accountant” and an accounting firm as “an entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant.”

A money services business (MSB) is defined as “a person or entity referred to in paragraph 5(h) of the Act.” That is, a person or entity who engages in the following activities:

- 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).

An accountant/accounting firm conducting a transfer on behalf of its client would not be considered to also be operating as an MSB. However, should an accountant/accounting firm provide MSB activities outside of its services as an accountant/accounting firm then it would be required to also register as an MSB.

5. Subsection 34(2) of the PCMLTFR indicates that “subsection (1) does not apply in respect of an accountant when they engage in any of the activities referred to in paragraph (1)(a) or (b) on behalf of their employer.” This subsection does not make any reference to accounting firms, only accountants. The PCMLTFR defines an accountant as “a chartered accountant, a certified general accountant or a certified management accountant”. Therefore, this subsection only applies to accountants who engage in the triggering activities on behalf of their employer.

Additionally, subsection 34(2) of the PCMLTFR is specific to accounting activities carried out on behalf of an employer. It is a question of fact to be able to determine whether an accountant is an employee. In fact, contract employment does not automatically suggest a legal employer/employee relationship. To assist you in your determination, the Canada

Revenue Agency's (CRA) standards, used to determine employment status for tax purposes, may be useful for assessing employment status within Canada.

Date answered: 2015-04-28

PI Number: PI-6303

Activity Sector(s): Accountants

Obligation(s): Other

Guidance: FIN-1, FIN-2

Regulations: 34(1), 34(2)

Act: 5(h), 5(j)

20.3 **Policy Interpretation PI No. 4542 answered on 2009-03-09: On exchange rates - Bank of Canada**⁴⁶²

If a transaction is conducted in a foreign currency or virtual currency, the amount of the transaction shall be converted into Canadian dollars using (a) the exchange rate that is published by the Bank of Canada for that foreign currency or virtual currency and that is in effect at the time of the transaction; or (b) if no exchange rate is published by the Bank of Canada for that foreign currency or virtual currency, the exchange rate that the person or entity would use in the ordinary course of business at the time of the transaction.

Question:

If the Bank of Canada doesn't list a particular currency then do we allow the RE to use an alternate site to obtain the exchange rate to determine reportable transactions?

Answer:

As per subsection 2(a) of PCMLTFA regulations – the conversion into Canadian dollars is based on the official conversion rate of the Bank of Canada. If there is no official conversion rate set out for that currency by the Bank of Canada, then yes the entity can rely on another alternative

⁴⁶² FINTRAC, *Archived Policy Interpretations - Reporting*, August 20, 2021

reliable system to determine the exchange rate – subsection 2(b) indicates that the entity would use the conversion rate for that currency in the normal course of business and the normal course of business would certainly include alternatives systems for currency rates not listed by the Bank of Canada.

Date answered: 2009-03-09

PI Number: PI-4542

Activity Sector(s): Financial entities, Money services businesses

Obligation(s): Reporting

Guidance: 8

Regulations: 2(a), 2(b)

20.4 Policy Interpretation PI No. 6409 answered on 2016-03-30: On the existence of a corporation and ascertaining identity of clients⁴⁶³

Question:

What type of document is sufficient to prove the existence of the corporation? Also, please confirm that there is no requirement to re-identify our clients at closing?

Answer:

Every real estate broker or sales person is subject to Part 1 of the Proceeds of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTA) when they act as an agent in respect of the purchase or sale of real estate. When subject to the PCMLTFA, the real estate broker or sales representative must keep the following records:

- a. a receipt of funds record in respect of every amount that they receive in the course of a single transaction, unless the amount is received from a financial entity or a public body;
- b. client information record in respect of every purchase or sale of real estate; and

⁴⁶³ FINTRAC, *Archived Policy Interpretations - Record Keeping*, August 20, 2021

- c. where the receipt of funds record or the client information record is in respect of a corporation, a copy of the part of official corporate records that contains any provision relating to the power to bind the corporation in respect of transactions with the real estate broker or sales representative.

If the real estate broker or sales representative receives an amount of \$10,000 or more in cash in the course of a single transaction, then they must keep a large cash transaction record instead of the receipt of funds record.

Pursuant to subsection 59.2(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, for any of the records listed above, the real estate broker or sales representative must ascertain the identity of every person who conducts the transaction, and, in accordance with sections 65 and 66, respectively, confirm the existence of every corporation or entity other than a corporation on whose behalf the transaction is conducted. In the case of a corporation, the real estate broker or sales representative must also ascertain the name and address of the corporation, as well as the names of its directors.

As outlined in FINTRAC's Guideline 6B - Record Keeping and Client Identification for Real Estate, to confirm the existence of a corporation as well as the corporation's name and address, a reporting entity may refer to the following documents:

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

When a real estate broker or sales representative is also required to keep a record a copy of the part of the official corporate records showing the provisions relating to the power to bind the corporation regarding the transaction, FINTRAC has suggested referring to a certificate of incumbency, the articles of incorporation or the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

If there were changes subsequent to the articles or bylaws that relate to the power to bind the corporation regarding the purchase and these changes were applicable at the time that the record had to be kept, then the board resolution stating the change would be included in this type of record.

You will note that the examples provided in the FINTRAC Guidelines are different for each requirement (confirmation of existence vs. power to bind the corporation), however should there be one document that does meet both requirements, then a real estate broker or sales person would be able to use this.

Regarding your question on ascertaining identification, as outlined above, a real estate broker or sales person is required to ascertain identity in relation to the keeping of certain records. In addition, identity must be ascertained, with some exceptions, if the real estate broker or sales person is filing a large cash or suspicious transaction report. If the real estate broker or sales person refers to the client's birth certificate, driver's licence, provincial health insurance card (if such use of the card is not prohibited by the applicable provincial law), passport or other similar document, then at the time this document is referred to, it must be valid and not have expired. There is not a specific requirement to ascertain the identity of your client again at closing, unless another obligation triggers such a requirement (i.e., receipt of funds, large cash transaction, client information record, etc.) If one of these other obligations triggers the need to ascertain identity again at closing, and should the real estate broker or sales person refer to the client's birth certificate, driver's licence, provincial health insurance card (if such use of the card is not prohibited by the applicable provincial law), passport or other similar document, then that document must be valid and not have expired.

Date answered: 2016-03-30

PI Number: PI-6409

Activity Sector(s): Real estate

Obligation(s): Record Keeping

Guidance:

Regulations: 1(2), 39(1), 59.2(1)

Act: Part 1

20.5 Policy Interpretation PI Number: PI-4606 modified on 2020-09-25: On length of being a PEFP and maintaining records⁴⁶⁴

Question:

We have said that once a PEFP always a PEFP (s 63(5)). This said, however, for how long would a RE have to keep the prescribed information regarding a PEFP? According to 69(1)(c), the answer is 5 years, however, does that conflict with 63(5) “once a PEFP always a PEFP”? Would the RE have to keep the information on a PEFP indefinitely?

Answer:

The records must be retained five years regardless of which record we are talking about.

The adage “once a PEFP always a PEFP” should be read as saying you are a PEFP even if you are deceased. Therefore, your children and other members of your family designated as PEFPs are still PEFP even though the original PEFP is deceased.

However, part of the RE’s risk-based approach would be that the RE may want to keep that information longer/or in storage as one never knows when the daughter of a deceased PEFP may open an account with the CU at some time and that information sure would be useful.

Date answered: 2009-06-24

PI Number: PI-4606

Activity Sector(s): Financial entities

Obligation(s): Politically Exposed Persons or Heads of an international organization

Guidance: Regulations: 69(1)(c), 63(5)

Date Modified: 2020-09-25

⁴⁶⁴FINTRAC, *Archived Policy Interpretations - Politically Exposed Persons or Heads of an international organization*, August 20, 2021

20.6 Policy Interpretation PI Number: PI-11075 Date answered: 2020-12-15: On PEP – source of cash or funds⁴⁶⁵

Question:

Are REs listed in subsection 120.1(3) of the amended Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) now obliged to establish the source of funds (which is broader than cash) when they receive \$100,000 or more in cash or virtual currency from a politically exposed person, the head of an international organization, or the family members and close associates?

Answer:

Currently pursuant to subsection 1(2) of the PCMLTFR:

- Cash means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada pursuant to the *Bank of Canada Act* that are intended for circulation in Canada or coins or bank notes of countries other than Canada.
- Funds means either:
 - a. cash; or
 - b. currency, securities, negotiable instruments or other financial instruments, in any form, that indicate a person's or entity's title or right to, or interest in, them.

Pursuant to the amended subsection 1(2) of the PCMLTFR, effective June 1, 2021:

- Cash means coins referred to in section 7 of the *Currency Act*, notes issued by the Bank of Canada under the *Bank of Canada Act* that are intended for circulation in Canada or coins or bank notes of countries other than Canada.
- Funds means:
 - cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or
 - a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

⁴⁶⁵ FINTRAC, *Archived Policy Interpretations - Politically Exposed Persons or Heads of an international organization*, August 20, 2021

For greater certainty, it does not include virtual currency.

- Virtual currency means:
 - A digital representation of value that can be used for payment or investment purposes, that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
 - A private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

In addition, pursuant to the amended PCMLTFR, effective June 1, 2021:

- 120.1(3) A British Columbia notary public, British Columbia notary corporation, accountant, accounting firm, real estate broker or sales representative, real estate developer, dealer in precious metals and precious stones or department or agent of Her Majesty in right of Canada or agent or mandatary of Her Majesty in right of a province shall take reasonable measures to determine whether a person from whom they receive an amount of \$100,000 or more, in cash or in virtual currency, is a politically exposed foreign person, a politically exposed domestic person or a head of an international organization, or a family member — referred to in subsection 2(1) — of, or a person who is closely associated with, one of those persons.
- 122.1(2) A person or entity that determines under subsection 120.1(3) that a person is a politically exposed foreign person or a family member — referred to in subsection 2(1) — of, or a person who is closely associated with, a politically exposed foreign person shall:
 - a. take reasonable measures to establish the source of the funds or virtual currency used for the transaction and the source of the person's wealth; and
 - b. ensure that a member of senior management reviews the transaction.

As can be seen above, the definition of “Cash” remains the same, the definition of “Funds” has been amended to account for digital fiat currencies, and a definition of “Virtual currency” has been added.

Where a reporting entity (RE) determines that the person from whom it receives \$100,000 or more in cash or virtual currency is a foreign PEP, family member or close associate, then it is required to take reasonable measures to establish the source of the funds or virtual currency used for that transaction. In a scenario where the \$100,000 transaction is solely made up of cash, there is no need to consider the source of other types of funds not used in

the transaction. However, in a scenario where the RE receives \$100,000 in cash, plus any additional amount(s) in another form of funds, the RE would be required to determine the source of **all funds** that were part of the transaction. As such, while it is \$100,000 cash that triggers the obligation to determine source of funds, it is all of the funds in that transaction for which reasonable measures must be taken to determine their source

Date answered: 2020-12-15

PI Number: PI-11075

Activity Sector(s): Accountants, British Columbia notaries, Dealers in precious metals and stones, Real estate

Obligation(s): Politically Exposed Persons or Heads of an international organization

Regulations: ss. 1(2), 120.1(3), 122.1(2)

Act: s. 9.3

20.7 Policy Interpretation PI Number: PI-11073 Date answered: 2020-12-09: PEP – Members of the same board⁴⁶⁶

Question:

Does simply being on the same board as a politically exposed person (PEP) make an individual a close business or personal associate. It is common practice for Boards to recruit members specifically because of their independence from other Board members and the corporation. How strictly does FINTRAC view the idea that all those on the same Boards as PEPs should be considered close business or personal associates?

Answer:

Pursuant to subsection 9.3(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), reporting entities are required to determine whether they are dealing with:

⁴⁶⁶FINTRAC, *Archived Policy Interpretations - Politically Exposed Persons or Heads of an international organization*, August 20, 2021

1. a foreign PEP, a prescribed family member of a foreign PEP, or a person who the person or entity **knows or should reasonably know is closely associated, for personal or business reasons**, with a foreign PEP;
2. a domestic PEP, a prescribed family member of a domestic PEP, or a person who the person or entity **knows or should reasonably know is closely associated, for personal or business reasons**, with a domestic PEP; or
3. the head of an international organization (HIO), a prescribed family member of a HIO, or a person who the person or entity **knows or should reasonably know is closely associated, for personal or business reasons**, with a HIO.

The term “close associate” is not defined further within the PCMLTFA or its associated Regulations. However, FINTRAC’s guidance clarifies that a close associate can be an individual who is closely connected to a PEP or HIO for personal or business reasons. The term “close associate” is not intended to capture every person who is associated with a PEP or HIO. For this reason, a reporting entity will need to have a means to determine if this is a close association they need to identify and treat as such.

Therefore, a reporting entity is not required to automatically consider every member of a board that a PEP/HIO is on to be a close associate, but has to take reasonable measures to determine whether they are dealing with a close associate of a PEP/HIO. The reasonable measures to be taken must be outlined in their compliance program’s policies and procedures.

Date answered: 2020-12-09

PI Number: PI-11073

Activity Sector(s): Financial entities, Life insurance, Money services businesses, Securities dealers

Obligation(s): Politically Exposed Persons or Heads of an international organization

Act: ss. 9.3(1)

20.8 Policy Interpretation PI Number: PI-11067 Date answered: 2020-11-26: Accountants – When are there requirements?⁴⁶⁷

Question:

I work for a Quebec municipality, and I am a member of the Quebec CPA Order. If a taxpayer decides to pay municipal taxes in cash and the amount is over \$10,000, do we have to fill out a Large Cash Transaction Report?

Am I required to do so as a mandatory of Her Majesty or as an accountant?

Answer:

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) applies to accountants, British Columbia notaries, casinos, dealers in precious metals and stones, life insurance companies, life insurance brokers or agents, money services businesses, real estate brokers or sales representatives, securities dealers and financial entities. Under subsection 1(2) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* (the Regulations), “financial entity” means a bank that is regulated by the *Bank Act*, an authorized foreign bank, as defined in section 2 of that Act, in respect of its business in Canada, a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial Act, an association that is regulated by the *Cooperative Credit Associations Act*, a financial services cooperative, a credit union central, a company that is regulated by the *Trust and Loan Companies Act* and a trust company or loan company that is regulated by a provincial Act. It includes a department or an entity that is an agent or mandatory of Her Majesty in right of Canada or of a province when it is carrying out an activity referred to in section 45.

Note that, under paragraph 5(l) of the PCMLTFA, departments and agents or mandataries of Her Majesty in right of Canada or of a province that are engaged in the business of accepting deposit liabilities, that issue or sell money orders to, or redeem them from, the public or that sell prescribed precious metals, while carrying out a prescribed activity, are subject to Part 1 of the PCMLTFA. In accordance with section 45 of the Regulations, every department and agent or mandatory of Her Majesty in right of Canada or of a province is also subject to Part 1 of the PCMLTFA when they accept deposit liabilities in the course of providing financial services to the public.

⁴⁶⁷ FINTRAC, *Archived Policy Interpretations - Other*, August 20, 2021

FINTRAC is of the view that taxes collected by any level of government are not deposit liabilities because the government agency that receives them is not responsible for remitting their amount to the person or entity; and for consistency with the wording of Canadian tax legislation, specifically, paragraph 123(1)(r.2) of the Excise Tax Act, debt collection services are not considered to be financial services.

Accordingly, when municipal governments collect taxes, they do not fall under the definition of agents or mandataries of the Crown subject to the PCMLTFA and its Regulations.

In addition, it is important to note that, under subsection 1(2) of the Regulations, “accountant means a chartered accountant, a certified general accountant or a certified management accountant.” Pursuant to subsection 34(1) of the Regulations, every accountant and every accounting firm is subject to Part 1 of the PCMLTFA when they

- a. engage in any of the following activities on behalf of any person or entity, namely,
 - i. receiving or paying funds,
 - ii. purchasing or selling securities, real properties or business assets or entities, or
 - iii. transferring funds or securities by any means; or
- b. give instructions on behalf of any person or entity in respect of any activity referred to in paragraph (a).

However, under subsection 34(2) of the Regulations, subsection (1) does not apply in respect of an accountant when they engage in any of the activities referred to in paragraph (1)(a) or (b) on behalf of their employer.

The above shows that accountants are not subject to the PCMLTFA and its Regulations simply because they are accountants, but that they are subject to them when they engage in certain activities. Consider, for example, an employee of a Municipality [sic], who is working as a Chartered Professional Accountant (CPA). Because the accountant is acting on behalf of the employer, the Municipality [sic], the accountant is not subject to the PCMLTFA and its Regulations as a CPA and thus does not have to meet the requirements for accountants set out in the PCMLTFA.

That said, FINTRAC has a mechanism for the general public to provide voluntary information about suspicions of money laundering or the financing of terrorist activities. For more information, please visit the FINTRAC website.

Date answered: 2020-11-26

PI Number: PI-11067

Activity Sector(s): Accountants

Obligation(s): Other

Act: 5(j), 5(l)

CHAPTER 21

Appendix G – Suspicious transaction report form

21.1 STR form, FINTRAC

This form is available at <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/STR-eng.pdf> or can be found on FINTRAC's Reporting Forms website at: <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng>.

21.2 STR instructions⁴⁶⁸

When to submit a suspicious transaction report (STR) to FINTRAC

Pursuant to subsection 9(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, “the person or entity shall send the report to the Centre as soon as practicable after they have taken measures that enable them to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.”

These measures include:

- screening for and identifying suspicious transactions
- assessing the facts and context surrounding the suspicious transaction

⁴⁶⁸These instructions are a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC, *Reporting suspicious transactions to FINTRAC*, August 12, 2021.

- linking ML/TF indicators to your assessment of the facts and context
- explaining your grounds for suspicion in an STR, where you articulate how the facts, context and ML/TF indicators allowed you to reach your grounds for suspicion

After completing the measures that enabled you to determine that you have reasonable grounds to suspect (RGS) that a transaction is related to the commission of an ML/TF offence, you must submit an STR to FINTRAC [as soon as practicable](#). These measures must be described in your [compliance policies and procedures](#).

As soon as practicable is interpreted to mean that you have completed the measures that have allowed you to determine that you reached the RGS threshold and as such the development and submission of that STR must be treated as a priority. FINTRAC expects that you are not giving unreasonable priority to other transaction monitoring tasks and may question delayed reports. The greater the delay, the greater the need for a suitable explanation. STRs can be complex, yet you must treat them as a priority and ensure they are timely; you must also complete the measures that enabled you to conclude that you have RGS the transaction is related to the commission of an ML/TF offence before you submit the report to FINTRAC.

There is no monetary threshold associated with the reporting of a suspicious transaction and under the Canadian anti-money laundering and anti-terrorist financing (AML/ATF) regime, STRs may contain transactions that must be submitted to FINTRAC in other types of reports. For example, if a completed transaction reported in an STR involved the receipt of cash from a client of \$10,000 or more, you would also be required to report this transaction to FINTRAC in a large cash transaction report (LCTR).

Service provider agreements

A service provider can submit and correct STRs on your behalf. However, as the reporting entity, you are ultimately responsible for meeting your obligations under the PCMLTFA and associated regulations, even if a service provider is reporting on your behalf. This legal responsibility cannot be delegated.

21.2.1 How to submit STRs

If you have a computer and an internet connection, you must submit STRs to FINTRAC electronically. You must submit by paper if you do not have the technological capacity to send an STR electronically.

Electronic reporting

There are two options for electronic reporting that provide for secure encrypted transmission that ensures your data's confidentiality and integrity. These two electronic reporting options are listed below.

- FINTRAC's secure website - FINTRAC web reporting
- batch file transfer

For more information about FINTRAC's electronic reporting system enrolment, see the electronic reporting page.⁴⁶⁹

FINTRAC web reporting is a secure application accessed through the Internet that allows you to manually submit individual reports, as well as correct them if needed. It is geared towards reporting entities with lower reporting volumes. **To report STRs electronically**, you must be enrolled and logged in to the FINTRAC web reporting system. For more information on FINTRAC web reporting, see the following document:

- FINTRAC web reporting:⁴⁷⁰ for instructions on how you can enroll in web reporting and the browser requirements

Batch reporting is a secure process that allows for the submission and correction of multiple reports (up to 10,000) in 'batch files' that are formatted according to FINTRAC's specifications. To use the batch reporting system, FINTRAC will provide you with batch transmission software but you will also need to enroll in FINTRAC web reporting and apply for a public key infrastructure (PKI) certificate. For more information on batch reporting, see the following links and documents:

- How can I use batch reporting?⁴⁷¹ for instructions on how you can enroll in FINTRAC web reporting and apply for a PKI certificate.
- Batch transmitting guide:⁴⁷² to assist you with installing and configuring the batch transmission software and to instruct you in how to transmit batch files to FINTRAC.

469 FINTRAC, *Electronic reporting*, June 1, 2021

470 FINTRAC, *Web reporting system*, November 4, 2021

471 FINTRAC, *Batch reporting*, September 28, 2021

472 FINTRAC, *Batch transmitting guide*, August 16, 2019

- Batch documentation:⁴⁷³ to assist you with how to create, submit and correct batch files.

Paper reporting

FINTRAC's STR paper reporting form can be printed from the [reporting forms](#) webpage or you can request a form to be faxed or mailed to you by calling FINTRAC at 1-866-346-8722.⁴⁷⁴

To ensure that the information provided is legible and to facilitate data entry, it would be preferable if the free-text areas of the STR (parts G and H) were completed using word-processing equipment. For reports completed by hand, please use black ink and CAPITAL LETTERS.

There are two ways you can send a completed paper STR form to FINTRAC:

- by fax: 1-866-226-2346, or
- by mail to the following address
Financial Transactions and Reports Analysis Centre of Canada
Section A
234 Laurier Avenue West, 24th floor
Ottawa, ON K1P 1H7
Canada

There is no official acknowledgement of receipt when you send a completed paper STR form to FINTRAC. However, FINTRAC will contact you and request that you resubmit electronically if you have the capability to do so.

21.2.2 Review and validation of reports by FINTRAC

FINTRAC reviews each report that is submitted to ensure that mandatory information is provided as per the PCMLTFA and associated regulations. There are three types of validation rules that FINTRAC uses to validate reports and these rules are described below.⁴⁷⁵

- presence – is there an entry in the field?
- format – is the entry in the correct structure?
- content – is the correct information entered in the appropriate field?

473 FINTRAC, [Batch reporting](#), September 28, 2021

474 FINTRAC, [Reporting forms \(paper reporting\)](#), July 23, 2021

475 FINTRAC, [Batch reporting](#), September 28, 2021

FINTRAC validation rules identify possible reporting problems or information gaps but do not cover all scenarios. While FINTRAC conducts a review of report submissions to assess the quality of reports, you should have your own proactive quality assurance practices independent of FINTRAC's review and validation of reports.

The report validation processes for FINTRAC web reporting and batch are different. Each report validation process is described in more detail below.

FINTRAC web reporting report validation

Reports submitted through FINTRAC web reporting are immediately validated by the application. FINTRAC web reporting will indicate where information is missing, incorrect or improperly formatted. You must correct all errors for mandatory fields before you can submit a report.

Batch report validation

Once a batch file has been submitted, FINTRAC validates the batch file against the validation rules. If there is an error with the structure or format of the file then you will receive a "Rejected" message and the batch file and reports within it will not be processed any further. **You must correct and resubmit the entire batch file.** Once you resubmit a batch file, it is revalidated against all validation rules.

If there is a potential issue in a reporting field then you may also receive a "Warning" message. If you receive a "Warning" message, the report has been accepted by FINTRAC but you should review the information submitted for accuracy and completeness.

Once your batch file has been accepted and validated, FINTRAC will send you a batch "Acknowledgement" message that will include the validation rule number(s) for any report(s) that require further action and any warning messages.

See FINTRAC's Standard Batch Reporting Instructions and Specifications for more information.⁴⁷⁶

⁴⁷⁶ FINTRAC, *Batch reporting*, September 28, 2021

21.2.3 Completing the STR form

FINTRAC's expectations for completing an STR

It is your responsibility to ensure that the information provided in an STR is complete and accurate. Your compliance policies and procedures must include details on the process for how you identify, assess and submit STRs to FINTRAC. It is possible that your organization has an automated or triggering system that detects unusual or suspicious transactions that would require assessment by a person to determine if you must submit an STR. A person with the appropriate knowledge and training is expected to be able to determine whether a transaction is related to the commission of an ML/TF offence. It is also important to note that the value of the transaction is not always the most important aspect of an STR. Training employees to perform this function is considered to be part of your compliance program obligations.⁴⁷⁷

Please note, an employee of a reporting entity can report a suspicious transaction to FINTRAC when:

- they have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence
- their employer did not or will not report

This stipulation is in place to cover the rare instances where an employee suspects that the threshold to report has been reached and their employer did not or will not send an STR. No person or entity will be prosecuted for sending an STR in good faith or for providing FINTRAC with information about suspicions of money laundering or terrorist financing.⁴⁷⁸ To submit an STR in this scenario, you may use the paper report form. For more information, please see field completion instructions to submit STRs by paper.⁴⁷⁹

It is important to FINTRAC's analysis process and disclosure recipients that the STRs you submit are comprehensive and of high quality. In Part G or H of the STR, it is important to **avoid jargon or non-public references**, such as terms and acronyms that are specific to your organization. Please consider an outside reader and use simple, clear and concise language.

A variety of information is often collected as part of an assessment to determine if you are required to submit an STR and this information is valuable to include in your report to FINTRAC. A well-completed STR should consider the following questions:

⁴⁷⁷ FINTRAC, *Guidance Glossary*, May 4, 2021

⁴⁷⁸ FINTRAC, *Reporting suspicious transactions to FINTRAC, footnote #2*, August 12, 2021

⁴⁷⁹ FINTRAC, *Reporting suspicious transactions*, August 12, 2021

1. **Who** are the parties to the transaction?
 - List the **conductor, beneficiary and holders** of all accounts involved in the transaction.
 - Take **reasonable measures** to verify the identity of the conductor of the transaction.⁴⁸⁰ This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.⁴⁸¹
 - Provide **identifying information** on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients.
 - **List owners, directors, officers and those with signing authority, when possible.** If the transaction involves an entity, you could include information on the ownership, control and structure of the business in the STR.
 - Provide **clear information about each person or entity's role** in each of the financial transactions described. It is important to know who is sending and receiving the funds⁴⁸² and this may be relevant in Part G of the STR.
 - **Explain the relationships among the persons or entities (if known).** This is very helpful to FINTRAC when trying to establish networks of persons or entities suspected of being involved in the commission or attempted commission of an ML/TF offence.
2. **When** was the transaction completed/attempted? If it was not completed, why not?
 - Provide the **facts, context and ML/TF indicators** regarding the transaction.
3. **What** are the financial instruments or mechanisms used to conduct the transaction?
4. **Where** did this transaction take place?
5. **Why** are the transaction(s) or attempted transaction(s) related to the commission or attempted commission of an ML/TF offence?
 - State the ML/TF indicators used to support your suspicion.
 - State the suspected criminal offence related to ML/TF, if known.
6. **How** did the transaction take place?

480 FINTRAC, *Reporting suspicious transactions to FINTRAC, footnote #3*, August 12, 2021

481 FINTRAC, *Reporting suspicious transactions to FINTRAC, footnote #4*, August 12, 2021

482 FINTRAC, *Guidance Glossary*, May 4, 2021

Once you have reached RGS, you must keep reporting as long as the suspicion remains. You are expected to periodically re-assess the client to verify that the level of suspicion has not changed. This process may be part of your documented risk assessment⁴⁸³ or ongoing monitoring.⁴⁸⁴ If you continue to report STRs on the same person or entity, you can reference a previous STR in Part G by:

- entering the FINTRAC STR number and date of submission
- providing the reasonable grounds to suspect (facts, context and ML/TF indicators) that were included in the first STR submission
- providing any new additional information

If you are reporting STRs because the assessment has changed due to new facts, context and/or ML/TF indicators, you are expected to provide them. For example, through the course of your assessment, you may have identified new ML/TF indicators or new parties transacting with your client. You may choose to include that information under a separate heading in part G so that it is properly labeled as new information.

You must keep a copy of all STRs submitted to FINTRAC for a period of at least five years after the day the report is sent.⁴⁸⁵ For more information on your record keeping obligations related to STRs, see your sector specific record keeping⁴⁸⁶ guidance.

You are not allowed to inform anyone, including the client, of the contents of an STR, or that you have made or will make such a report, if the intent is to prejudice a criminal investigation. This applies whether such an investigation has begun or not.⁴⁸⁷ It is important to not tip off your client about the fact that you are making a suspicious transaction report. Therefore, you should not be requesting information that you would not normally request during a transaction.

STR submission limitations

Each STR must include at least one transaction and may include up to 99 transactions as long as all the transactions:

- have the same transaction status (e.g., all completed transactions or all attempted transactions); and
- took place at the same location.

483 FINTRAC, *Risk assessment guidance*, August 4, 2021

484 FINTRAC, *Ongoing monitoring requirements*, August 4, 2021

485 FINTRAC, *Reporting suspicious transactions, footnote #5*, February 10, 2022

486 FINTRAC, *Record keeping*, March 23, 2021

487 FINTRAC, *Reporting suspicious transactions, footnote #6*, August 12, 2021

For example, someone brings a money order for \$6,000 CAD and successfully sends an electronic funds transfer for \$6,000 CAD (**first completed transaction**). Later that day, the same person returns to the same location and brings \$5,000 CAD cash and receives a money order (**second completed transaction**). In this case, if there are reasonable grounds to suspect that the two completed transactions, conducted at the same location, are related to the commission or attempted commission of an ML/TF offence, you should provide the transaction details for the two transactions in the same STR. **While the transactions may be referenced in part G as part of the facts, context and/or ML/TF indicators, the transaction details themselves must be entered in parts B1 through F.**

In a situation where related suspicious transactions took place at **different locations**, an STR must be submitted **for each location** and only detail the transactions that occurred at that specific location. In addition, all transactions should have the same status as either completed or attempted to be included in a single report.

If you have more than 99 transactions to report at one time, you must submit the additional transaction(s) in a separate STR. You cannot insert a spreadsheet or include the additional transactions in part G of the STR. If the information is available, you can reference related STRs in part G by entering the FINTRAC STR number and date of submission.

Common STR deficiencies to avoid

The following are examples of deficiencies that FINTRAC has identified through its assessments and other compliance activities. FINTRAC is sharing these examples to illustrate common errors that you can avoid.

- **Using a higher threshold as your basis for reporting:** You are required to submit an STR when you have completed the measures that enable you to establish that there are **reasonable grounds to suspect** that a transaction is related to the commission of an ML/TF offence. This means that there is a **possibility** of an ML/TF offence and that you **do not** have to prove the facts or information that led to your suspicion.

In some cases, it is possible that you have determined that there are **reasonable grounds to believe** that the transaction is related to the commission or attempted commission of an ML/TF offence. Reasonable grounds to believe means that there are verified facts that support the **probability** that an ML/TF offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe, not just suspect**, that an ML/TF offence has occurred.

If you identify a transaction whereby you reach reasonable grounds to believe that an ML/TF offence has occurred, you **must** begin an assessment of the related transactions immediately as you have surpassed the RGS threshold. If assessed by FINTRAC and there are reasonable grounds to believe that a transaction is related to the commission of an ML/TF offence, and you have not begun an assessment of the facts, context or ML/TF indicators, you may be cited for not submitting an STR.

- **Failing to list all the transactions and accounts relevant to your suspicion in parts B through F:** You are required to report all the transactions and accounts in parts B through F that led to your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. Providing a summary of the transactions in part G is not enough.
- **Not listing or naming all parties to the transactions when the information is available:** All parties to the transaction must be listed, including third-parties.⁴⁸⁸ You should also specify whether the parties are known or unknown. This has been observed in transactions involving multiple parties such as wire transfers. For example, if you are reporting a wire transfer, you should include any information you have regarding both the ordering client and beneficiary. This could include (but is not limited to) their names, their account number and institution, their relationship, and any known identifiers. FINTRAC acknowledges that this information may not always be at your disposal, but when you know it, it should be provided.
- **Part G does not elaborate on your grounds for suspicion or link them to the transactions reported in parts B through F:** You are required to articulate the reasons for your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence in an STR. This includes providing all of the relevant facts, context and ML/TF indicators related to the transactions reported in parts B through F that support your suspicion in part G. This deficiency has been observed when a reporting entity does not articulate the reasons for their suspicion or does not explain how or why certain information is relevant to their suspicion.

21.2.4 Field completion instructions

Note: Unless otherwise stated, this section details specific instructions that **apply to both electronic and paper reporting.**

⁴⁸⁸FINTRAC, *Guidance Glossary*, May 4, 2021

Parts of a suspicious transaction report

STRs contain eight specific parts:

- **Part A: Information about where the transaction took place**

In part A of the STR, you must provide information about you as the reporting entity, and about the physical location where the completed or attempted suspicious transaction took place.

When completing part A it is important to note that:

- **reporting entity's full name** is your entity's full legal name. Even if you have entered into a contractual relationship with another entity to conduct transactions on your behalf, it is your name that **must** be entered into this field.
- **reporting entity number** is the number that was assigned to you when you enrolled in FINTRAC web reporting.
- **reporting entity location number** is the location number where the transaction took place or was attempted. If you have multiple locations, your FINTRAC web reporting administrator is responsible for adding the other locations, as well as maintaining the location information.
- **reporting entity report reference number** is a unique internal reference number generated by your entity. The recording of the internal reference number on the STR may help you to quickly identify the report if required to at a later date.
- **activity sector** is the type of business and/or activities you undertake.

- **Part B1: Information about how the transaction was initiated**

In part B1 of the STR, you must provide the date of the transaction, the transaction amount, the detail of the funds involved in initiating the transaction, how the transaction was conducted, as well as information on any other institution, entity or individual that was involved in the transaction.

When completing part B1 it is important to note that:

- the date of transaction is the date that the transaction occurred. Whereas, the date of posting is the date on which the funds from the transaction are received in an account
- you must provide (if applicable) the name of any other person or entity or the name and number of the other institution **involved in the initiation of** the transaction

If you need to report more than one transaction in an STR, a separate part B1 will have to be completed for each transaction.

Part B1, field 8* **Other institution name** and **number**, or any **other person or entity** will be masked once received by FINTRAC. This field has been removed from the paper form.

- **Part B2: Information about how the transaction was completed**

In part B2 of the STR, you must detail:

- how the funds were used in the completed transaction or how they were going to be used in an attempted transaction
- whether the individual who conducted or attempted the suspicious transaction did so on anyone else's behalf

The funds in a transaction may have been used in several ways, therefore resulting in more than one disposition⁴⁸⁹ having to be detailed in your STR. For example, your client may initiate a transaction in cash, then use some of the funds to send an electronic funds transfer (disposition 1), order a bank draft (disposition 2) and deposit the remaining funds (disposition 3). If there is more than one disposition, you will need to complete a separate part B2 for each disposition.

Part B2, field 15* **Other institution name** and **number**, or any **other person or entity** will be masked once received by FINTRAC. This field has been removed from the paper form.

- **Part C: Account information, if the transaction involved an account**

In part C of the STR, you must provide the account details for each disposition that involved an account (completed transaction) or was going to involve an account (attempted transaction), if applicable. For example, if the related disposition was a “deposit”, this part is required.

- **Part D: Information about the individual conducting the transaction**

In part D of the STR, you must provide information about the individual who completed or attempted to complete the transaction.

⁴⁸⁹FINTRAC, *Guidance Glossary*, May 4, 2021

If more than one transaction is reported in an STR, a **separate part D** will have to be completed **for each transaction**.

- **Part E: Information about the entity on whose behalf the transaction was conducted**

In part E of the STR, if applicable, you must provide information about the entity on whose behalf the transaction was conducted or attempted.

Part E needs to be completed if you indicated in part B2 that the transaction was conducted “on behalf of an entity.”

A separate part E must be completed for **each** disposition that was conducted or attempted on behalf of an entity.

- **Part F: Information about the individual on whose behalf the transaction was conducted**

In part F of the STR, if applicable, you must provide information about the individual on whose behalf the transaction was conducted or attempted.

Part F must be completed if you indicated in part B2 that the transaction was conducted “On behalf of another individual.”

A separate part F must be completed for each disposition that was conducted or attempted on behalf of another individual.

- **Part G: Description of suspicious transaction and any facts or context associated with the suspicion**

This section is the narrative that explains your grounds for suspicion and should include the results of your assessment of facts, context and ML/TF indicators that led to your decision to submit an STR to FINTRAC. The narrative should include the explanation of this assessment and should not assume that the reader will be familiar with acronyms or terminology specific to your business. Detailed and high quality STRs provide valuable and actionable intelligence for FINTRAC, and this section is shared with law enforcement and intelligence agencies in FINTRAC disclosures.

The narrative provided in this section should focus on the question: “Why do you think the transaction is suspicious of ML/TF?”

The following are examples of the type of information that, when available, have been provided in STRs and have contributed greatly to FINTRAC’s analysis:

- any client identification information not already captured in the transaction details listed in part B, i.e., known aliases or nicknames
- additional contact information (phone numbers, email addresses, etc.)
- details for credit card activity including details of purchases (dates, amounts, retailer (online or in-store) and details of payments (dates, amounts, conductor and source of payment)
- details for electronic transfers (such as e-mail money transfers, wire transfers) including IP addresses and sender/recipient email addresses
- location of ATM withdrawals
- any related STR number(s) and the date(s) previously submitted
- the history the client has with you
- links made to other people, businesses and accounts
- information on the ownership, control and structure of an entity that is not already captured in part B, particularly for any business entities that have a complex structure
- the intended or expected use of an account versus the activity you may have observed
- any other information about your interactions with the client
- the ML/TF indicators or factors that assisted in forming the basis of your suspicion
- any information, including publicly available information and/or information from law enforcement, that made you suspect distinctly that the transaction might be related to terrorist financing, money laundering, or both
- any details surrounding why an attempted transaction was not completed
- any context or clarification about the information that was reported in the structured sections (Parts B through F)

FINTRAC has been able to identify networks of suspected money launderers and terrorist financiers through pieces of information such as email addresses and secondary identifiers (nicknames) or phone numbers. This type of information may seem insignificant but can be very important to FINTRAC, as it may identify connections among persons, entities or crimes when compared against other FINTRAC intelligence.

It is important that your narrative is consistent with the information in parts B through F of the STR form. For example, if you are referring to specific account activity in this section the details of those accounts and transactions should be entered in the structured fields. It is also important that you do not

refer to any internal files or documents since FINTRAC cannot have access to these internal files or documents for its analysis. It is also not possible to see graphics, underlined, italicized or bolded text included in an STR.

- **Part H: Description of action taken**

Describe any actions taken by you, in addition to reporting to FINTRAC, in response to the suspicious transaction.

Examples of additional actions that you may take include:

- reporting the information directly to law enforcement
- initiating enhanced transaction monitoring
- closing the account(s) in question or exiting the business relationship
- cancelling, reversing or rejecting the transaction

Reporting an STR to FINTRAC does not prevent you from contacting law enforcement directly. **However, even if you do contact law enforcement directly about your suspicions of money laundering or terrorist financing, you must still submit an STR to FINTRAC.** Some STRs have included the law enforcement agency's contact information in part H of the STR when the information was reported directly to law enforcement and this information can be helpful.

Standardized field instructions

This section includes standardized instructions for the level of effort that is required for certain fields as well as standard instructions for completing fields for identification, addresses, telephone numbers and occupation.⁴⁹⁰

1. **Each field within an STR is categorized as either mandatory, mandatory if applicable, or reasonable measures.**

- a. Mandatory:

- » Mandatory fields require you to obtain the information to complete the STR and will be marked with an asterisk (*).
- » However, in the case of an **attempted transaction**, you are to take reasonable measures⁴⁹¹ to obtain the information for any mandatory field.

- b. Mandatory, if applicable:

- » Mandatory if applicable fields must be completed if they are applicable to you or the transaction being reported. If applicable, you must provide the information if you obtained it at the time of the transaction, or if it is contained within your institution.

⁴⁹⁰FINTRAC, *Guidance Glossary*, May 4, 2021

⁴⁹¹FINTRAC, *Guidance Glossary*, May 4, 2021

- » These fields will be indicated with both an asterisk (*) and “(if applicable)” next to them.
- c. Reasonable measures:
 - » For all other fields that do not have an asterisk, you must take reasonable measures to obtain the information.
 - » Reasonable measures can include asking for the information as long as you don’t think it will tip off the person that you are submitting an STR.
 - » Reasonable measures also means that you must provide the information if you obtained it, or if it is contained within your institution.

Note: In certain circumstances a required report field may not be applicable. Do not enter “N/A” or “n/a” or substitute any other abbreviations, special characters (e.g., “x”, “-” or “**”) or words (e.g., unknown) in these fields. They are to be left blank.

2. **Client identification**

If you used the dual-process method to identify a person, you only need to provide the details of one of the identifiers. You can use your judgement to determine which identifier would be most advantageous to FINTRAC analysis. Please note that a Social Insurance Number (SIN) must not be reported to FINTRAC.

The record keeping requirement for the dual-process method includes the source of the information, so FINTRAC expects the issuing jurisdiction and country to align with the source of the information, but would only expect, as per the validation rules, that the reporting entity include the country of issue for the dual-process method.

In addition, you cannot use a provincial health card for identification purposes where it is prohibited by provincial legislation.

For more information on how to identify persons and examples of acceptable photo identification documents, refer to FINTRAC’s guidance on Methods to verify the identity of persons and entities.⁴⁹²

3. **On behalf of indicator**

Applies to part B2 of an STR.

⁴⁹² FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021 and Chapters 23 and 24 of this guide.

You are required to take reasonable measures to determine if there is another person or entity instructing your client to conduct an activity or a transaction. Reasonable measures include asking your client if they are acting on someone else's instructions or retrieving the information that may already be contained in your records.

When determining whether an individual has conducted or attempted a suspicious transaction on anyone else's behalf, it is not about who owns or benefits from the money, or who is carrying out the transaction or activity, but rather about **who gives the instructions** to handle the money or conduct the transaction or particular activity.

If you determine that a third-party was instructing your client, then you must indicate if the transaction was conducted on behalf of an entity or on behalf of another person.

If there is no third-party, or you were not able to determine whether there is a third-party, then indicate that this part is not applicable.

4. **Address fields**

Applies to the following fields of an STR:

- a. A3* - A6* (mandatory)
- b. D5 - D9
- c. D20 - D24
- d. E3 - E7
- e. F4 - F8
- f. F19 - F23

The complete physical address includes the street number, street name, the city, province, and country. If there is no province or state applicable to the address, leave this field blank.

Please note that the following **are not valid addresses** and **should not** be provided:

- a. a post office box without a complete physical address (e.g., PO Box 333)
- b. a general delivery address or
- c. only a suite number (e.g., Suite 256) without additional address information

It is possible that some of the examples above may be included in part G of the STR because they are relevant but they are not considered a valid address in terms of the client identification.

In cases where the person or entity resides in an area where there is no street address, provide a detailed description which clearly describes the physical location. For example, in these unique cases you could enter “the third house to the right after the community center” as the street address where a person lives.

A legal land description can be acceptable so long as the legal land description is specific enough to pinpoint the physical location of where the client lives. If the legal land description refers to an area or a parcel of land on which multiple properties are located, the legal land description would not be sufficient.

For persons who are transient (e.g., travelling in a recreational vehicle, temporarily working in a camp, etc.) and have no fixed address, you are required to provide the following:

- a. for Canadian residents, their permanent address is required, even if that is not where they are currently residing;
- b. for non-Canadian residents travelling in Canada for a short period of time, their foreign residential address is required; and
- c. for non-Canadian residents living in Canada for a longer period of time (e.g., a student), then the person’s temporary Canadian address should be provided.

5. **Telephone number fields**

Applies to the following fields of an STR:

- a. A10* - A10A
- b. D11
- c. D18 - D18A
- d. D25 - D25A
- e. E8 - E8A
- f. F9
- g. F10 - F10A
- h. F24 - F24A

If the telephone number is from Canada or the United States, enter the area code and local number (e.g., 999-999-9999).

If the telephone number is from outside Canada or the United States, enter the country code, city code and local number using a dash (-) to separate each one. For example, ‘99-999-9999-9999’ would indicate a two-digit country code, a three-digit city code and an eight-digit local number.

6. **Occupation fields**

Applies to the following fields of an STR:

- a. D17
- b. F17

When entering a person's occupation information, you must be as descriptive as possible. For example:

- a. If the person is a manager, the occupation provided should reflect the area of management, such as "hotel reservations manager" or "retail clothing store manager."
- b. If the person is a consultant, the occupation provided should reflect the type of consulting, such as "IT consultant" or "forestry consultant."
- c. If the person is a professional, the occupation provided should reflect the type of profession, such as "petroleum engineer" or "family physician."
- d. If the person is a labourer, the occupation provided should reflect the type of labour performed, such as "road construction worker" or "landscape labourer."
- e. If the person is not working, the occupation provided should still be as descriptive as possible, such as "student", "unemployed" or "retired".

CHAPTER 22

Appendix H - Sample receipt of funds record and instructions

Requirements: All fields on the receipt of funds record are mandatory. You must record:⁴⁹³

- the date of the receipt
- if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation
- if the amount is received from or on behalf of an entity, the entity's name and address and the nature of its principal business
- the amount of the funds received and of any part of the funds that is received in cash
- the method by which the amount is received
- the type and amount of each fiat currency involved in the receipt
- if applicable, the exchange rates used and their source
- the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder
- the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth
- every reference number that is connected to the transaction and has a function equivalent to that of an account number
- the purpose of the transaction

⁴⁹³ PCMLTFR subsection 1(2)

If the receipt of funds record is about a client that is a corporation,⁴⁹⁴ you must also keep a copy of the part of the official corporate records that contains any provision relating to the power to bind the corporation regarding the transaction. Official records can include a certificate of incumbency, the articles of incorporation or the bylaws of the corporation that set out the officers duly authorized to sign on the behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.⁴⁹⁵

If there were changes subsequent to the articles or bylaws that related to the power to bind the corporation regarding the transaction, and these changes were applicable at the time the transaction was conducted, then the board resolution stating the change would be included in this type of record.

Table 20

Sample receipt of funds record

RECEIPT OF FUNDS RECORD			
The following information must be collected, retained and recorded for each prescribed transaction where the organization receives funds (not including virtual currency) with a value of CAD \$3,000 or more from a client in respect of triggering activities.			
INFORMATION ON THE PERSON FROM WHOM YOU RECEIVED THE FUNDS			
Last name		First name	
Street address			Apartment/unit #
City	Prov.	Postal code	
Date of birth	Nature of principal business or occupation		
INFORMATION WHEN AMOUNT IS RECEIVED FROM OR ON BEHALF OF AN ENTITY			
Name of entity		Nature of principal business	
Street address			Apartment/unit #
City	Prov.	Postal code	
INFORMATION ON ALL OTHER PERSONS INVOLVED IN THE TRANSACTION			
Last name		First name	
Street address			Apartment/Unit #
City	Prov.	Postal Code	
Date of birth	Nature of principal business or occupation		

494 PCMLTFR paragraph 52(b)

495 See Section 20.4 of this guide for FINTRAC's Policy Interpretation PI-6409 dated 2016-03-30

INFORMATION ON ALL OTHER ENTITIES INVOLVED IN THE TRANSACTION		
Name of other entities		
Street address		Apartment/unit #
City	Prov.	Postal code
Nature of principal business		
TRANSACTION INFORMATION		
Date of the receipt	Amount	
Type of each fiat currency	Amount of each fiat currency	
If applicable, exchange rate	If applicable, source of exchange rate	
Purpose, details and type of transaction	Other persons or entities involved	
Method by which amount received	What part of funds received were in cash?	
INFORMATION ON EVERY ACCOUNT AFFECTED BY THE TRANSACTION, IF APPLICABLE		
Account #	Type of account	
Accountholder's full name		
Every reference number connected to the transaction that is equivalent to account number		
INFORMATION, IF APPLICABLE		
If the receipt of funds record is about a corporation, you also need to keep a copy of the part of the official corporate records showing the provisions relating to the power to bind the corporation regarding the transaction.		

Instructions on completing the receipt of funds record

Information on the person providing the funds should be included on this form and be as specific as possible. Specifically:

- The address should be their physical location and not a PO Box.
- The occupation should be as specific as possible and should avoid vague occupations such as “self-employed,” “consultant” and “import export.”
- The purpose of the transaction should explain the whole transaction such as “received funds from client to wire.”
- If the funds are in cash form, this should be explained using such wording as “in person” “mailed” or “courier.”
- The sections on accounts would be applicable if the funds were received in a form other than cash. For instance, if the client gave you a cheque, the account information related to that cheque should be recorded.

- The section on entity information would be applicable if the client is not an individual. In that case, information on the individual conducting the transaction on behalf of the entity and the information on the entity would both be required. If the client is an entity that is incorporated, a copy of their record that binds them to the transaction must kept.

CHAPTER 23

Appendix I – Verifying the identity of a person

23.1 Requirement

A person's identity must be verified when any of the following occur as part of an engagement for which triggering activities have occurred:

- receipt of funds of \$3,000 or above
- large cash transaction and large virtual currency transaction
- suspicious transaction report (reasonable measures without tipping off)
- terrorist property report (reasonable measures)

You do not need to verify a person's identity for subsequent transactions or activities, as required, if you have already verified the identity of the person using one of the methods explained in this guide and as referenced in FINTRAC's guidance;⁴⁹⁶ or the methods specified in the PCMLTFR prior to June 1, 2021 as it read at the time, and have kept the required record. You must not have doubts about the information that was previously used to verify the person's identity. If you have doubts, you must verify their identity again using the methods explained in this guide and as referenced in FINTRAC's guidance.⁴⁹⁷

⁴⁹⁶ FINTRAC, *When to verify the identity of persons and entities – Accountants*, and PCMLTFR subsection 155(1)

⁴⁹⁷ Ibid

23.2 Methods of verifying the identity

When dealing with an entity, both the entity and the individual conducting the transaction on the entity's behalf must be identified.

The AML/ATF legislation allows the use of one of four different methods of verifying a person's identity for accountants and accounting firms.⁴⁹⁸ For greater clarity, a fifth method is only applicable to reporting entities covered under the PCMLTFA under paragraphs 5(a) to 5(g) which does not include accountants and accounting firms. The four methods are:

1. government-issued photo identification method
2. credit file method
3. dual-process method
4. reliance method

The AML/ATF legislation also allows you to verify the identity of a person when relying on an agent or mandatary, as long as one of the four identification methods described above are used and by meeting certain conditions.

In all cases, a document that you use to verify the identity of a person must be authentic, valid and current.⁴⁹⁹ Other information that is used for that purpose must be valid and current.

Authentic is defined as:⁵⁰⁰ In respect of a government-issued photo identification document that is used to verify identity, is genuine and has the character of an original, credible and reliable document issued by the competent authority (federal, provincial, territorial government).

Valid is defined as:⁵⁰¹ In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes.

498 PCMLTFR paragraphs 105(1)(a) to (d) and FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

499 PCMLTFR subsection 105(5)

500 FINTRAC, *Guidance glossary*, May 4, 2021

501 FINTRAC, *Guidance glossary*, May 4, 2021

Current is defined as:⁵⁰² In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified.

Reminder: The identity of the person must be verified at the time of the transaction.

23.3 Government-issued photo identification method⁵⁰³

One method of verifying the identity of a person under the AML/ATF legislation⁵⁰⁴ is to refer to government-issued photo identification document.⁵⁰⁵ To do so, the document must:

- be authentic, valid and current⁵⁰⁶
- be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document)
- indicate the person's name
- include a photo of the person
- include a unique identifying number
- match the name and appearance of the person being identified

Photo identification documents issued by municipal governments, Canadian or foreign, are not acceptable. See Section 23.3.4 of this guide or FINTRAC's guidance⁵⁰⁷ for acceptable government-issued photo identification documents.

You can determine whether a government-issued photo identification document is **authentic, valid and current** by viewing it **in person**, and by looking at the characteristics of the original physical document and its security features (or markers, as applicable) **in the presence of the person being identified**. This will allow you to be satisfied that it is authentic, as issued by the competent authority (federal, provincial or territorial government), valid (unaltered, not counterfeit) and current (not expired).

502 FINTRAC, *Guidance glossary*, May 4, 2021

503 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

504 PCMLTFR paragraph 105(1)(a)

505 PCMLTFR subsection 105(5)

506 Ibid

507 FINTRAC, *Methods to verify the identity of persons and entities, Annex 4*, August 4, 2021

23.3.1 Use of the government-issued photo identification method if a person is not physically present

You may use the government-issued photo identification method if a person is **not physically present**, but you must have a **process in place to authenticate** the government-issued photo identification document. For instance, you could assess a document by using a technology capable of determining the document's authenticity. For example, you could:

- ask a person to scan their government-issued photo identification document using the camera on their mobile phone or electronic device
- use a technology to compare the features of the government-issued photo identification document against known characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) to be satisfied that it is an authentic document as issued by the competent authority (federal, provincial, or territorial government)

When a person **is not physically present**, you must still determine whether the authenticated government-issued photo identification document is **valid** and **current**, and that the name and photo are those of the person providing the document. For example, you could:

- participate in a live video chat session with the person and compare the name and the features of the live video image to the name and photo on the authentic government-issued photo identification document, or
- ask the person to take a “selfie” photo using the camera on their mobile phone or electronic device and use an application to apply facial recognition technology to compare the features of that “selfie” to the photo on the authentic government-issued photo identification document. You would also need a process to compare the name on the government-issued photo identification document with the name provided by the person

Note: It is not enough to only view a person and their government-issued photo identification document through a video conference or another type of virtual application.

Your compliance program's policies and procedures must describe the processes you follow to determine whether a government-issued photo identification document is authentic, whether the client is present or not, and how you will confirm that it is valid and current. Your policies and procedures must also describe the steps you use to confirm that the name

and photograph are those of the person. Your processes to determine that a government-issued photo identification document is authentic, valid, and current, **and** the verification step (ensuring that the name and photo match the name and appearance of the person), do **not** need to happen at the same time. It is up to you to determine the timing, but you must complete both steps.

23.3.2 Record keeping requirements for the government-issued photo identification method

If you use the government-issued photo identification method, you must record:⁵⁰⁸

- the person’s name
- the date on which you verified the person’s identity
- the type of document used (for example, driver’s licence, passport, etc.)
- the unique identifying number of the document used
- the jurisdiction (province or state) and country of issue of the document
- the expiry date of the document, if available (if this information appears on the document or card, you must record it)

23.3.3 Sample record when using the government-issued photo identification method

Table 21

REFERRING TO AN IDENTIFICATION DOCUMENT WITH NAME AND PHOTOGRAPH	
Last name	First name
ID type * <input type="checkbox"/> Driver’s licence <input type="checkbox"/> Passport <input type="checkbox"/> Other (specify)	
Unique identifying number of the ID type	Expiry date (If available)
Issuing jurisdiction	Country of issue
Name of accountant confirming client identity:	
Date on which the person’s identity was verified:	
* The document must be authentic, valid and current; issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document); indicate the person’s name; include a photo of the person; include a unique identifying number; and match the name and appearance of the person being identified.	

508 PCMLTFR paragraph 108(a)

23.3.4 Examples of acceptable photo identification documents⁵⁰⁹

The following list provides examples of acceptable government-issued photo identification documents from federal, provincial or territorial authorities. This is not an exhaustive list.

Type of card or document	Issuing province or state and country
Canadian passport	Canada
Permanent resident card	Canada
Citizenship card (issued prior to 2012)	Canada
Secure Certificate of Indian Status	Canada
Driver's licences	
British Columbia Driver's Licence	British Columbia, Canada
Alberta Driver's Licence	Alberta, Canada
Saskatchewan Driver's Licence	Saskatchewan, Canada
Manitoba Driver's Licence	Manitoba, Canada
Ontario Driver's Licence	Ontario, Canada
Québec Driver's Licence	Quebec, Canada
New Brunswick Driver's Licence	New Brunswick, Canada
Nova Scotia Driver's Licence	Nova Scotia, Canada
Prince Edward Island Driver's Licence	Prince Edward Island, Canada
Newfoundland and Labrador Driver's Licence	Newfoundland and Labrador, Canada
Yukon Driver's Licence	Yukon, Canada
Northwest Territories Driver's Licence	Northwest Territories, Canada
Nunavut Driver's Licence	Nunavut, Canada
DND 404 Driver's Licence	Department of National Defence, Canada
Provincial services cards	
British Columbia Services Card	British Columbia, Canada
Provincial or territorial identity cards	
British Columbia Enhanced ID	British Columbia, Canada
Alberta Photo Identification Card	Alberta, Canada
Saskatchewan Non-driver photo ID	Saskatchewan, Canada
Manitoba Enhanced Identification Card	Manitoba, Canada
Ontario Photo Card	Ontario, Canada
New Brunswick Photo ID Card	New Brunswick, Canada
Nova Scotia Identification Card	Nova Scotia, Canada

⁵⁰⁹FINTRAC, *Methods to verify the identity of persons and entities*, Annex 4, August 4, 2021

Type of card or document	Issuing province or state and country
Prince Edward Island Voluntary ID	Prince Edward Island, Canada
Newfoundland and Labrador Photo Identification Card	Newfoundland and Labrador, Canada
Northwest Territories General Identification Card	Northwest Territories, Canada
Nunavut General Identification Card	Nunavut, Canada
Types of card or international document	
Global Entry Card	United States
NEXUS	United States or Canada
France driver's licence	France
Australian passport	Australia
Pennsylvania driver's licence	Pennsylvania, United States

* Note: You cannot use a provincial health card for identification purposes where it is prohibited by provincial legislation to use the card as a form of identification or to record the health card number.

23.4 Credit file method

Another method of verifying a person's identity is to use the credit file method. The AML/ATF legislation allows you to refer⁵¹⁰ to information that is in the person's credit file, if it:

- contains information that is **valid and current**⁵¹¹
- is from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable)
- has been in existence for at least three years
- contains information that is derived from more than one source (i.e., more than one tradeline)
- matches the name, address and date of birth of the person being identified

A credit file provides a rating on a person's ability to repay loans; however, it is possible to request a credit file to verify a person's identifying information that does not include a credit assessment. You do not need a credit

510 PCMLTFR paragraph 105(1)(c)

511 PCMLTFR subsection 105(5)

assessment to verify the identity of a person. Equifax Canada and TransUnion Canada are Canadian credit bureaus that provide credit file information for identification purposes.

To use the credit file method, you must conduct the search **at the time** you are verifying the person's identity. A person cannot provide you with a copy of their credit file, nor can a previously obtained credit file be used.

It is acceptable to use an automated system to match the person's information with the information in the person's credit file. You may also refer to a third-party vendor to provide you with valid and current information from the person's credit file. A third-party vendor is a business that is authorized by a Canadian credit bureau to provide access to Canadian credit information.

If any of the information provided by the person (name, address or date of birth) does not match the information in the credit file, you cannot use that credit file to verify the identity of the person. You will need to use another credit file from a different provider (credit bureau or third-party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.

On occasion, information found in the credit file may contain a variation on the name or a discrepancy in the address that was provided to you by the person. In these instances, you must determine whether the information in the credit file matches the information provided by the person. For example:

- If there is a slight typo in the address or name, you may determine that the information still matches what the person provided.
- If there is a discrepancy in their date of birth, it is more likely that you will determine that the information does not match.
 - In this case, if this is your determination, you cannot rely on the information in the credit file for identification purposes. You will need to use another credit file from a different provider (credit bureau or third-party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.
- If there are multiple addresses in the credit file, it is possible that the address the person provided to you is not the primary address in the credit file, but it does appear in the credit file as a secondary address. If this is the case, you can still meet your requirements for ensuring that the information matches what the person provided.

23.4.1 Record keeping requirements for the credit file method

If you use the credit file method, you must record:⁵¹²

- the person's name
- the date you consulted or searched the credit file
- the name of the Canadian credit bureau or third-party vendor as the source holding the credit file
- the person's credit file number

Your compliance program's policies and procedures must describe the processes you follow to verify a person's identity using the credit file method **and** how you will ensure that the information is valid and current. It should also include the steps you will take if the information is not valid and current (for example, search a different credit file, use another method, stop the transaction, etc.).

A sample record is provided in Section 23.4.2 of this guide. Below are some examples of what to do if the information in the credit file does not precisely match the name or address provided:⁵¹³

- If there is a slight typo in the address or name, you may determine that the information still matches what the individual provided.
- If there is a discrepancy in their date of birth, it is more likely that you will determine that the information does not match.
 - In this case, if this is your determination, you cannot rely on the information referred to in the credit file for identification purposes. An alternative source or method (government-issued photo identification document or dual process) to verify the individual's identity must be used.
- If there are multiple addresses in the credit file, it is possible that the address that the individual provided to you is not the primary address in the credit file but does appear in the credit file as a secondary address. It is possible that this may still meet your requirements for ensuring that the information matches what the individual provided.

Your compliance program's policies and procedures must describe the processes you follow to use the credit file method to verify an individual's identity and how you will ensure that the information is valid and current.

512 PCMLTFR paragraph 108(c)

513 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

It should also include the steps you will take if the information is not valid and current (for example, search a different credit file, use another method, stop the transaction, etc.).

23.4.2 Sample record when referring to information in a client's credit file

Table 22

REFERRING TO INFORMATION IN A CLIENT'S CREDIT FILE*		
You must confirm that the name, address, and date of birth in the credit file are those of the person		
Last name	First name	
Home address		Apartment/Unit #
City	Prov./Terr.	Postal code
Date of birth		
Name of the Canadian credit bureau or third-party vendor as the source holding the credit file		
Credit file number		
Name, address and date of birth match those of the person <input type="checkbox"/>		
Name of accountant confirming client identity:		
Date the credit file was consulted or searched:		
* You may only use the information from that credit file if it contains information that is valid and current; is from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable); has been in existence for at least three years; contains information that is derived from more than one source (i.e., more than one tradeline); and matches the name, address and date of birth of the person being identified.		

23.5 Dual-process method⁵¹⁴

Another method of verifying the identity of a person is referring to information using a dual-process method. The AML/ATF legislation⁵¹⁵ allows you to use this method when **you refer to two of three** sources of information. You may use any two of the following:

1. referring to information from a reliable source that includes the **person's name and address**, and confirming that the name and address are those of the person

514 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

515 PCMLTFR paragraph 105(1)(d)

2. referring to information from a reliable source that includes the **person's name and date of birth**, and confirming that the name and date of birth are those of the person, or
3. referring to information that includes the **person's name and confirms that they hold a deposit account, a prepaid payment product account or a credit card or other loan account with a financial entity** and confirming that information

The information you refer to **must** be valid and current⁵¹⁶ **and** come from two different reliable sources. This information could be found in **statements, letters, certificates, forms or other information sources** that can be provided through an original version or by another version of the information's original format such as a fax, a photocopy, a scan, or an electronic image. For example, you can rely on a fax, photocopy, scan or electronic image of a government-issued photo identification document as one of the two pieces of information required to verify a person's identity.

You **cannot** use the same source for the two categories of information you choose to verify a person's identity.⁵¹⁷ you cannot rely on a bank statement from Bank A that includes the person's name and address and another bank statement from Bank A that includes the person's name and confirms that the person holds a deposit account, as Bank A would be the same source of both categories of information. You can, however, refer to a bank statement from Bank A that contains the person's name and confirms that the person holds a deposit account, and rely on an electronic image of a driver's licence to confirm the person's name and address.

For further precision, the possible combinations for this method include:

- Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's name and **date of birth** and confirming that this matches the information provided by the person.
OR
- Referring to information from one reliable source that includes the **person's name** and address and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name and a**

516 PCMLTFR subsection 105(5)

517 PCMLTFR subsection 105(4)

financial account (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

OR

- Referring to information from one reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and a **financial account** (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

Note: If the information does not match the information provided by the person, you cannot rely on it. For example, it is **not acceptable** to rely on information if the account number or number that is associated with the information is truncated or redacted. On occasion, information from a source may contain a variation on the name of the client or a typo in the client's address. In these instances, you must determine whether the information matches the information provided by the person. If it is a slight typo in the address or a misspelled name, you may determine that the information still matches what the person provided. However, in the case of an incorrect date of birth, it is more likely that you will determine that the information does not match. In this case, you cannot rely on the information from this source for identification purposes. You must obtain information from a different source under the dual-process method or use a different method (for example, the government-issued photo identification method or the credit file method) to verify the person's identity.

23.5.1 What is a reliable source of information?

A reliable source is an originator or issuer of information that you trust. To be considered reliable, the source should be well known and considered reputable. For example, a reliable source could be the federal, provincial, territorial or municipal levels of government, Crown corporations, federally regulated financial institutions, or utility providers.⁵¹⁸

If you have already verified the identity of an individual, you do not need to re-verify it upon subsequent transactions, unless you have doubts about the accuracy of the information that was used at the time of verification.

⁵¹⁸ FINTRAC, *Methods to verify the identity of persons and entities*, Annex 5, August 4, 2021 (table outlining examples of reliable sources of information for the dual-process method) or refer to Section 23.5.4 of this guide.

23.5.2 How to use a credit file under the dual-process method to verify the identity of an individual

A Canadian credit file can be used as one of the two sources of information required to verify the identity of an individual. It can be used to verify the individual's name and address, name and date of birth, or to confirm the person's name and confirm that the person has a credit card account or loan account. If you use a credit file as one of the information pieces for the dual-process method, it must have existed for at least six months.⁵¹⁹

Information from a second source, for example, a property tax assessment, must be used to confirm the second category of information under the dual-process method. In this instance, the two reliable sources are the Canadian credit bureau that provided the credit file information and the municipal government that issued the property tax assessment. The information from these two sources must match the information provided by the person.

You can also refer to information from a Canadian credit bureau if it acts as an aggregator that compiles information from different reliable sources (often referred to as tradelines). In this instance, the Canadian credit bureau must provide you with information from **two** independent tradelines where each tradeline confirms one of the two categories of information required to verify the identity of a person under this method. In this instance, each tradeline is a distinct source; the credit bureau is not the source.

The tradelines cannot be your own, as the RE verifying the person's identity, and each tradeline must originate from a different reliable source (for example, a federally regulated financial institution, a utility service provider, etc.).

23.5.3 Record keeping requirements for the dual-process method

If you use the dual-process method to verify a person's identity, you must record:⁵²⁰

- the person's name
- the date you verified the information
- the name of the two different reliable sources that were used to verify the identity of the person
- the type of information referred to (for example, a utility statement, a bank statement, a marriage licence)

519 PCMLTFR subsection 105(4)

520 PCMLTFR subsection 108(d)

- the number associated with the information (for example, account number or if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, etc.). If you use information aggregated by a Canadian credit bureau and receive information from two distinct sources (tradelines), you must record the account number or number associated to each tradeline, not the aggregator (credit bureau) number.

Your compliance program’s policies and procedures must describe the processes you follow when using the dual-process method to verify a person’s identity and how you will ensure that the information is valid and current.

23.5.4 Sample record when referring to information using the dual method

Table 23

REFERRING TO INFORMATION USING THE DUAL METHOD			
You must choose any two of the three combinations below			
<p>Note: The source of information that is referred to in these combinations must not be from, or derived from, the same source and neither the person whose identity is being verified nor the Accountant or Accounting Firm that is verifying the person’s identity can be a source. If information in a credit file is referred to, the credit file must have been in existence for at least six months.</p>			
COMBINATION 1 - NAME AND ADDRESS/NAME AND DATE OF BIRTH			
<p>You must refer to information from one reliable source (A) that includes the person’s name and address and confirm that this matches the information provided by the person, and refer to information from a different reliable source (B) that includes the person’s name and date of birth and confirm that this matches the information provided by the person.</p>			
Last name	First name	Date of birth	
Home address		Apartment/Unit #	
City	Prov./Terr.	Postal code	
Name of reliable source A:		Name of reliable source B:	
Do you confirm that the name and address provided by the person matches the information obtained from reliable source A?			YES <input type="checkbox"/>
Do you confirm that the name and date of birth provided by the person matches the information obtained from reliable source B?			YES <input type="checkbox"/>
Name of accountant confirming client identity:			
Date the above information was confirmed:			

COMBINATION 2 - NAME AND ADDRESS/NAME AND FINANCIAL ACCOUNT

You must refer to information from one reliable source (A) that includes the person's **name** and **address** and confirm that this matches the information provided by the person, and refer to information from a different reliable source (B) that includes the person's **name** and a **financial account** (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirm this information.

Last name		First name	
Home address			Apartment/Unit #
City	Prov./Terr.		Postal code
Name of reliable source A:		Name of reliable source B:	
Confirm that the person holds one of the following types of financial account:			
Deposit account <input type="checkbox"/>	Prepaid payment product account <input type="checkbox"/>	Credit card <input type="checkbox"/>	Loan account <input type="checkbox"/>
Name of financial entity where account held:			
Account no. associated with it:			
Do you confirm that the name and address provided by the person matches the information obtained from reliable source A?			YES <input type="checkbox"/>
Do you confirm from reliable source B information that includes the person's name and financial account ?			YES <input type="checkbox"/>
Name of accountant confirming client identity:			
Date the above information was confirmed:			

COMBINATION 3 - NAME AND DATE OF BIRTH/NAME AND FINANCIAL ACCOUNT

You must refer to information from one reliable source (A) that includes the person's **name** and **date of birth** and confirm that this matches the information provided by the person, and referring to information from a different reliable source (B) that includes the person's **name** and a **financial account** (specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

Last name		First name		Date of birth
Name of reliable source A:			Name of reliable source B:	
Confirm that the person holds one of the following below				
Deposit account <input type="checkbox"/>	Prepaid payment product account <input type="checkbox"/>	Credit card <input type="checkbox"/>	Loan account <input type="checkbox"/>	
Name of financial entity where account held:				
Account no. associated with it:				
Do you confirm that the name and date of birth provided by the person matches the information obtained from reliable source A?				YES <input type="checkbox"/>
Do you confirm from reliable source B information that includes the person's name and financial account ?				YES <input type="checkbox"/>
Name of accountant confirming client identity:				
Date the above information was confirmed:				

23.5.5 Examples of reliable sources of information for the dual-process method

This is **not** an exhaustive list.⁵²¹ You must always rely on valid and current information whether it be through an original version or whether you obtain another version of the information's original format, such as a fax, photocopy, scan or electronic image and that can meet your related record keeping obligations.

521 This table is a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC. FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

Table 24

<p>Reliable sources of information to verify name and address</p>	<p>Reliable sources of information to verify name and date of birth</p>	<p>Reliable sources of information to verify name and confirm a financial account (specifically, a deposit account, prepaid payment product account, credit card account or loan account)</p>
<p>Issued by a Canadian government body:</p> <ul style="list-style-type: none"> • A fax, photocopy, scan or electronic image of a government-issued photo identification document • Any statement, form, certificate or other source issued by a Canadian government body (federal, provincial, territorial or municipal): <ul style="list-style-type: none"> – Canada Pension Plan (CPP) statement – property tax assessment issued by a municipality – provincially issued vehicle registration • Benefits statement: <ul style="list-style-type: none"> – federal, provincial, territorial, or municipal levels 	<p>Issued by a Canadian government body:</p> <ul style="list-style-type: none"> • A fax, photocopy, scan or electronic image of a government-issued photo identification document • Any statement, form, certificate or other source issued by a Canadian government body (federal, provincial, territorial or municipal): <ul style="list-style-type: none"> – birth certificate – marriage certificate or government-issued proof of marriage document (long-form which includes date of birth) – divorce documentation – permanent resident card – citizenship certificate – temporary driver's licence (non-photo) 	<p>Confirm that the person has a deposit account, prepaid payment product account, credit card or loan account by means of:</p> <ul style="list-style-type: none"> • Credit card statement • Bank statement for deposit or chequing accounts • Loan account statement (for example, mortgage) • Cheque that has been processed in the last statement period (cleared, insufficient funds) by a financial institution • Telephone call, email, letter, or other traceable means of confirmation from the financial entity holding the deposit account, prepaid payment product account, credit card or loan account • Product from a Canadian credit bureau (containing two trade lines in existence for at least six months) • Use of micro-deposits

Reliable sources of information to verify name and address	Reliable sources of information to verify name and date of birth	Reliable sources of information to verify name and confirm a financial account (specifically, a deposit account, prepaid payment product account, credit card account or loan account)
<p>Issued by other Canadian sources</p> <ul style="list-style-type: none"> • utility bill (for example, electricity, water, telecommunications) • Canada 411 • Record of Employment • registered investment account statements (for example, RRSP, TFSA or RRIF) • Canadian credit file that has been in existence for at least six months • product from a Canadian credit bureau or other third-party (containing two trade lines in existence for at least six months) • insurance documents (home, auto, life) • for a currently enrolled student, a transcript or documentation issued by a school that contains a unique reference number 	<p>Issued by other Canadian sources</p> <ul style="list-style-type: none"> • Canadian credit file that has been in existence for at least six months • product from a Canadian credit bureau (containing two trade lines in existence for at least six months) • investment account statements (for example, RRSP, GIC) • insurance documents (home, auto, life) 	
	<p>Issued by a foreign government</p> <ul style="list-style-type: none"> • travel visa 	

23.6 Reliance method⁵²²

Another method of verifying a person's identity is to use the reliance method. You may verify the identity of a person by relying on measures that were previously taken by **another reporting entity (RE)** (person or entity that is referred to in section 5 of the PCMLTFA);⁵²³ **or**

522 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021
523 PCMLTFR paragraph 107(1)(a)

To rely on measures previously taken by **another RE** to verify the identity of a person, you must:⁵²⁴

- As soon as feasible, obtain from the **other RE** the information that was confirmed as being that of the person, and be satisfied that:
 - the information is valid and current
 - the **other RE** verified the person's identity using the government-issued photo identification method, the credit file method or the dual-process method, or if the **other RE** verified the person's identity prior to June 1, 2021, that they did so in accordance with the AML/ATF Legislation, by using the methods that were in place at the time
- Have a written agreement or arrangement with the **other RE** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the person's identity.

23.6.1 Record keeping requirements for the reliance method

If you rely on **another RE** to verify the identity of a person, you must keep a record of:⁵²⁵

- the person's name
- the written agreement or arrangement with the **other RE** for the purpose of verifying a person's identity
- The information that the **other RE** referred to in order to verify the identity the person.

Your compliance program's policies and procedures must describe the processes you follow when using the reliance method to verify a person's identity and how you will ensure that the information is valid and current.

524 PCMLTFR subsection 107(3)
525 PCMLTFR subsection 108(i)

23.7 Summary of the methods to identify persons and associated record keeping obligations

Table 25

Identification method	Documents or information to review	Identification details that must match	Information that must be recorded
Government-issued photo identification	Photo identification document issued by a government (not a municipal government) that is authentic, valid and current	Name and photograph	<ul style="list-style-type: none"> • person's name • date of verification • type of document • document number • province or state and country that issued the document • expiry date (if applicable)
Credit file	Valid and current information from a Canadian credit file that has been in existence for at least three years where information is derived from more than one source	Name, address and date of birth	<ul style="list-style-type: none"> • person's name • date you consulted/ searched the credit file • name of the credit bureau or third-party vendor • person's credit file number
Dual-process	Valid and current information from two different reliable sources where neither the RE nor the person is a source	A combination of two of the following: <ul style="list-style-type: none"> • name and address • name and date of birth, or • name and confirmation of a financial account 	<ul style="list-style-type: none"> • person's name • date you verified the information • name of the two different sources used to verify the identity of the person • type of information referred to • account number or number associated with the information if no account number exists

Identification method	Documents or information to review	Identification details that must match	Information that must be recorded
Reliance	<ul style="list-style-type: none"> Be satisfied that the information from the other RE or affiliated foreign entity is valid and current and that the person's identity was verified by using the government-issued photo identification, credit file or dual-process methods. or Where the identity was verified prior to June 1, 2021, that the person's identity was verified using one of the methods in force in the PCMLTFR at that time. 	The identification details listed under the identification method used	<ul style="list-style-type: none"> person's name the written agreement or arrangement with the other RE or affiliated foreign entity for the purpose of verifying a person's identity the information provided by the other RE or affiliated foreign entity that they referred to in order to verify the identity of the person

23.8 You may also rely on an agent or mandatory to verify the identity of a person on your behalf

The AML/ATF legislation allows accountants or accounting firms to rely on measures that were previously taken by an agent or mandatory to verify the identity of a person as long as one of the three methods prescribed (government-issued photo identification method, the credit file method, or dual-process method) are used by the agent or mandatory and **if the agent or mandatory** was, at the time they took the measures.⁵²⁶

- acting in their own capacity, whether or not they were required to use the methods in accordance with the AML/ATF legislation, or
- acting as an agent or mandatory under a written agreement or arrangement that was entered into, with another RE, for the purposes of verifying a person's identity using either the government-issued photo

⁵²⁶ PCMLTFR subsections 106(1) and (2)

identification method, the credit file method or the dual-process method, or if the measures were taken prior to June 1, 2021, using the methods in accordance with the AML/ATF legislation that were in place at the time

To use an agent or mandatary to verify the identity of a person the AML/ATF legislation requires that three conditions must be met:⁵²⁷

- have in place a written agreement or arrangement **before** you use them
- obtain, as soon as feasible, all the information that the agent or mandatary referred to in order to verify the person's identity, and the information the agent or mandatary, confirmed as being that of the person
- Be satisfied that:
 - the information the agent or mandatary confirmed as being that of the person is valid and current
 - the person's identity was verified using the government-issued photo identification method, the credit file method or the dual-process method, or, if the person's identity was verified prior to June 1, 2021, using the methods in accordance with the AML/ATF legislation in place at the time

What is a written agreement or arrangement? You must have in place a written agreement or arrangement⁵²⁸ with the agent or mandatary for the purposes of verifying client identification in line with the AML/ATF legislation.⁵²⁹

As a best practice, an agent/mandatary agreement should explicitly state that the agreement is for the purpose of verifying client identification on behalf of the accountant or accounting firm under the obligations of the AML/ATF legislation. It should also describe what prescribed information or which of the AML/ATF legislation prescribed methods will be used to verify the identity. It should also obligate the agent/mandatary to remit to the accountant or accounting firm details collected in respect of each identification conducted.

As a best practice, it should set out what you expect from them and that you obtain from them the client identification information prior to the performance of the identification function. It is recommended that the effective date of the agreement and the signature of the agent/mandatary and the accountant or accounting firm also be included on the agreement. An agent or mandatary can be any individual or entity.

527 PCMLTFR subsection 106(3)
528 PCMLTFR paragraph 106(3)(a)
529 PCMLTFR subsection 105(1)

Obtain as soon as feasible. The information or the record that is required to be kept should be provided to the accountant or accounting firm without delay as the AML/ATF legislation imposes the obligation on the accountant or accounting firm to “as soon as feasible⁵³⁰, obtain from the agent or mandatary the information” that the agent or mandatary referred to in order to verify the person’s identity and the information that the agent or mandatary confirmed as being that of the person.

Be satisfied that the confirmed information you receive is valid and current. You must be satisfied that the information that the agent or mandatary confirmed as being that of the person is valid and current and that the agent or mandatary verified the person’s identity in the manner prescribed by the AML/ATF legislation⁵³¹ and described in Sections 23.3 to 23.7 of this guide or, if the measures were taken before June 1, 2021, that the agent or mandatary verified the person’s identity in accordance with the AML/ATF legislation, as it read at the time the measures were taken.

Your compliance program’s policies and procedures must describe the processes you follow when using the reliance method to verify a person’s identity and how you will ensure that the information is valid and current.

23.8.1 Examples of acceptable/not acceptable use of an agent or mandatary⁵³²

Example 1 — Acceptable: Jane Smith would like to open an account with you. Your agent – with whom you have a written agreement for this purpose – verified Jane Smith’s identity in 2019 using the government-issued photo identification method, by referring to her driver’s licence, which expired in February 2021. In 2019, Jane Smith’s name and appearance matched the name and photograph on the driver’s licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. Jane’s name and appearance have not changed. When you obtain the information from the agent, you are satisfied that the information the agent confirmed as being Jane’s (her name and photo) is still valid and current and is therefore acceptable. It does not matter that her licence (the identification document used by the agent) has expired, as it is the information that you must be satisfied is valid and current, not the document.

530 PCMLTFR paragraph 106(3)(b)

531 Specifically, PCMLTFR paragraphs 105(1)(a) to (d)

532 FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

Example 2 – NOT acceptable: Jane Smith (maiden name – Jane Rogers) would like to carry out a transaction for which you must verify her identity. Your agent – with whom you have a written agreement for this purpose – verified Jane Rogers’ identity in 2019 using the government-issued photo identification method, by referring to her driver’s licence, which has not yet expired. In 2019, Jane Rogers’ name and appearance matched the name and photograph on the driver’s licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. However, although the licence has not yet expired, it is not acceptable to rely on the information from the agent now because the agent will provide information on Jane Rogers, and she is now Jane Smith, so the information provided by the agent will not be valid and current.

Example 3 – NOT acceptable: Jane Smith would like to carry out a transaction for which you must verify her identity. Your agent – with whom you have a written agreement for this purpose – verified Jane Smith’s identity in 2019 by referring to her driver’s licence, which expired in 2018. In 2019, because Jane Smith’s driver’s licence had expired, her identity was not verified in accordance with the government-issued photo identification method. As such, it is not acceptable to rely on the information from the agent.

23.8.2 Record keeping when relying on an agent or mandatary⁵³³

When an agent/mandatary verifies the client’s identification under the agreement,⁵³⁴ a record should document the required client’s personal information as the prescribed methods in the AML/ATF legislation and described in Chapter 23 of this guide. Table 26 summarizes who can identify a person on your behalf.

When you verify the identity of a person by using an agent or mandatary, you must keep a record of:⁵³⁵

- the person’s name
- the written agreement or arrangement with the agent or mandatary for verifying a person’s identity

533 FINTRAC *Methods to verify the identity of persons and entities*, Annex 2, August 4, 2021

534 PCMLTFR paragraph 106(3)(a)

535 PCMLTFR paragraph 108(h)

- all the information the agent or mandatary referred to in order to verify the identity of the person, and the information that the agent or mandatary confirmed as being that of the person (this includes, as applicable, information that is required to be kept in the record for the method used)

Table 26

Who	Documents or information to review	Identification details that must match	Information that must be recorded
Agent or mandatary that: <ul style="list-style-type: none"> • acts for you • previously acted in their own capacity as an agent or mandatary under a written agreement or arrangement with another person or entity for the purposes of verifying identity 	Be satisfied that the information is valid and current and that the person's identity was verified using one of the government-issued photo identification, credit file or dual-process methods Or where the identity was verified prior to June 1, 2021, that person's identity was verified using one of the methods in force in the AML/ATF legislation at that time.	The identification details listed under the identification method used.	<ul style="list-style-type: none"> • person's name • the written agreement or arrangement with the agent or mandatary for the purpose of verifying a person's identity • all of the information the agent or mandatary referred to when verifying the person's identity • the information obtained from the agent or mandatary that they confirmed as being that of the person

23.9 Identifying a person less than 12 years old and a person less than 16 years old

The AML/ATF Legislation requires the identity of a person who is **under 12 years of age** to be verified by verifying the identity of one parent, guardian or tutor and record the parent, guardian or tutor's information.⁵³⁶ You can rely on the information provided by the parent, guardian or tutor in order to record the child's identification details.

536 PCMLTFR subsection 105(2)

If a child is **between 12 and 15 years of age**, you can verify their identity by using any of the methods. If this is not possible due to a lack of identification information, you may use a variation of the dual-process method that allows you to:

- refer to one reliable source of information that includes the name and address of the child's parent, guardian, or tutor⁵³⁷
- refer to a second reliable source that includes the child's name and date of birth

For example, if the child has a passport, you may be able to use it to verify their identity under the government-issued photo identification method. If not, you could rely on the parent's driver's licence to verify the parent's name and their common address, and the child's birth certificate to verify the child's name and date of birth.

23.10 Exceptions to the verification of the identity of a person

You do **not** need to verify a person's identity for subsequent transactions or activities, as required, **if** you have already verified the identity of the person using:⁵³⁸

- one of the methods explained in this guidance, or
- the methods specified in the PCMLTFR prior to June 1, 2021, as it read at the time, and have kept the required record

You must not have doubts about the information that was previously used to verify the person's identity. If you have doubts, you must verify their identity again using the methods explained in FINTRAC's guidance and in Chapter 23 of this guide.⁵³⁹

Note: In the context of a business merger or acquisition, you are not required to re-identify the acquired clients if their identities were verified in accordance with the methods in the PCMLTFR at the time the verification took place. As a best practice, you are encouraged to review and update client information (for example, name, address, occupation, etc.), in accordance with your risk assessment process. The acquired clients become the responsibility of

537 PCMLTFR subsection 105(3)

538 PCMLTFR subsection 155(1)

539 Ibid

the acquiring entity which must ensure compliance with the PCMLTFA and associated regulations. This includes reviewing any money laundering or terrorist financing risks that may be associated with these clients.

You do not have to identify an individual if you conduct a transaction in the following situations:⁵⁴⁰

- a. the sale of an *exempt policy* as defined in subsection 306(1) of the Income Tax Regulations⁵⁴¹
- b. the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component
- c. the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the *Pension Benefits Standards Act, 1985*,⁵⁴² or similar provincial legislation
- d. the sale of a registered annuity policy or a registered retirement income fund
- e. the sale of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy
- f. a transaction that is part of a reverse mortgage or structured settlement
- g. the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation
- h. the opening of an account in the name of an affiliate of a financial entity, if the affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Act
- i. the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account

540 PCMLTFR subsection 154(2)

541 Government of Canada, [Income Tax Regulations](#), subsection 306(1), January 10, 2022

542 Government of Canada, [Pension Benefits Standards Act, 1985](#), January 10, 2022

- j. the opening of an account established in accordance with the escrow requirements of a Canadian securities regulator or Canadian stock exchange or provincial legislation
- k. the opening of an account if the account holder or settlor is a pension fund that is regulated under federal or provincial legislation
- l. the opening of an account in the name of, or in respect of which instructions are authorized to be given by, a financial entity, a securities dealer, a life insurance company or an investment fund that is regulated under provincial securities legislation
- m. a public body
- n. a corporation or trust that has minimum net assets of \$75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the *Income Tax Act*⁵⁴³ and that operates in a country that is a member of the Financial Action Task Force
- o. a subsidiary of a public body referred to in paragraph (m) or a corporation or trust referred to in paragraph (n) whose financial statements are consolidated with the financial statements of that public body, corporation or trust, or
- p. the opening of an account solely in the course of providing accounting services to a securities dealer

You are not subject to the AML/ATF legislation as an accountant or accounting firm if the activities you undertake are in respect of an audit, review or compilation engagement, or carried out in accordance with the recommendations set out in the *CPA Canada Handbook*.

You do not have to identify an individual for the receipt of funds in an amount of \$3,000 or more, if the amount is received from a financial entity, public body or from a person who is acting on behalf of a client that is a financial entity or public body.

You do not have to identify the individual who conducts a large cash transaction if the cash is received from a financial entity or from a person who is acting on behalf of a client that is a financial entity or public body.⁵⁴⁴

⁵⁴³ Government of Canada, *Income Tax Act*, January 10, 2022
⁵⁴⁴ PCMLTFR section 48

If you determine that a person is a politically exposed foreign person or a family member, as it read at the time the determination was made, you are not required to make the determination again.⁵⁴⁵ For a description of the requirements when dealing with a **politically exposed person, their family members and close associates** refer to Chapter 15

545 PCMLTFR subsection 155(4)

CHAPTER 24

Appendix J – Verifying the identity of an entity

You can use any of the two methods described in this chapter to verify the identity of an entity:

- confirmation of existence method, or
- reliance method

While an entity can be a corporation, a trust, a partnership, a fund, or an unincorporated association or organization, corporations are subject to different requirements than other entities (as explained below).

24.1 Confirmation of existence method

The confirmation of existence method can be used to verify the identity of a corporation **or** an **entity other than a corporation**.

24.1.1 Corporation

To verify the identity of a corporation, you may refer to:⁵⁴⁶

- a certificate of incorporation
- a record that has to be filed annually under provincial securities legislation, or
- the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors, such as a certificate of active corporate status,

⁵⁴⁶ PCMLTFR subsection 109(1)

the corporation's published annual report signed by an audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government

The record you refer to must be authentic, valid and current.⁵⁴⁷

You may obtain a corporation's name and address and the names of its directors from a publicly accessible database, such as a provincial or federal database like the Corporations Canada database,⁵⁴⁸ or a corporation search and registration service through subscription.

When a corporation is a securities dealer, you do not need to confirm the names of its directors when you confirm its existence.⁵⁴⁹

24.1.2 Other than a corporation

To verify the identity of an entity other than a corporation, you may refer to:⁵⁵⁰

- a partnership agreement
- articles of association, or
- the most recent version of any other record that confirms its existence and contains its name and address

The record you refer to must be authentic, valid and current.⁵⁵¹

24.1.3 Record keeping requirements when verifying the identity of a corporation or other entity

If you refer to a paper record or an electronic version of a record, you must keep the record or a copy of it. If the electronic version of the record that you refer to is contained in a database that is accessible to the public, you must keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.⁵⁵²

Your compliance program's policies and procedures must describe the processes you follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how you will ensure that the information is authentic, valid and current.

547 PCMLTFR subsection 109(2)

548 Corporations Canada, [Search for a Federal Corporation](#)

549 PCMLTFR subsection 109(3)

550 PCMLTFR subsection 112(1)

551 PCMLTFR subsection 112(2)

552 PCMLTFR subsections 109(5) and 112(4)

24.2 Reliance method

The reliance method can be used to verify the identity of a corporation or an entity other than a corporation. This method means relying on the measures that were previously taken by another reporting entity (a person or entity that is referred to in section 5 of the PCMLTFA).⁵⁵³

24.2.1 Corporation or entity other than a corporation

To rely on the measures previously taken by **another reporting entity (RE)** to verify the identity of a corporation or other entity, you must:⁵⁵⁴

- As soon as feasible, obtain from the **other RE** the information that was used to confirm the identity of the corporation or other entity, as the case may be, and be satisfied that:
 - the information is valid and current
 - **for a corporation**, its identity was verified by the **other RE** by referring to a record as described in the confirmation of existence method above, **or** if the measures to verify the corporation's identity were performed prior to June 1, 2021, that the **other RE** confirmed the corporation's existence and ascertained its name, address, and the names of its directors in accordance with the methods in the PCMLTFR as they read at that time;⁵⁵⁵
 - **for an entity other than a corporation**, its identity was verified by the **other RE** by referring to a record as described in the confirmation of existence method above, or if the measures to verify the entity's identity were performed prior to June 1, 2021, the **other RE** confirmed the entity's existence in accordance with the methods in the PCMLTFR as they read at that time.⁵⁵⁶
- Have a written agreement or arrangement in place with the **other RE** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the identity of the **corporation** or other **entity**, as the case may be.⁵⁵⁷

Your compliance program's policies and procedures must describe the processes you follow when using the reliance method to verify the identity of corporations and other entities and how you will ensure that the information is valid and current.

553 PCMLTFR paragraphs 110(1)(a) and 113(1)(a)

554 PCMLTFR subsections 110(3) and 113(3)

555 PCMLTFR paragraph 110(3)(a)

556 PCMLTFR subsection 113(3)(a)

557 PCMLTFR paragraphs 110(3)(b) and 113(3)(b)

24.3 Summary of methods to identify an entity and associated record keeping obligations⁵⁵⁸

Table 27

Identification method	Documents or information to review	Identification details that must match	Information that must be recorded
Confirmation of existence	<ul style="list-style-type: none"> information that is authentic, valid and current <p>For an entity (other than a corporation):</p> <ul style="list-style-type: none"> partnership agreement articles of association the most recent version of any other record that confirms its existence and contains its name and address <p>For a corporation:</p> <ul style="list-style-type: none"> certificate of incorporation record that has to be filed annually under provincial securities legislation the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors 	<ul style="list-style-type: none"> name and address names of directors (for corporation only) 	<p>If you consulted an electronic record from a publicly accessible database:</p> <ul style="list-style-type: none"> registration number type of document consulted source of the electronic document <p>If you consulted a paper record or an electronic record:</p> <ul style="list-style-type: none"> the paper record, or a copy of the record

558 This table is a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC. FINTRAC, *Methods to verify the identity of persons and entities*, August 4, 2021

Identification method	Documents or information to review	Identification details that must match	Information that must be recorded
Reliance	<ul style="list-style-type: none"> Verify that information from the other RE or affiliated foreign entity is valid and current, and that the entity's identity was verified by using the confirmation of existence method. Where the identity was verified prior to June 1, 2021, that the entity's identity was verified using one of the methods in force in the PCMLTFR at that time. 	<ul style="list-style-type: none"> name and address names of directors (for corporation only) 	<ul style="list-style-type: none"> entity's name the written agreement or arrangement with the other RE or affiliated foreign entity for the purpose of verifying an entity's identity the information provided by the other RE or affiliated foreign entity that they referred to in order to verify the identity of the entity

24.4 Exceptions to record keeping for the verification of identity of an entity

You do not have to:

- Verify the existence of an entity for the receipt of funds in an amount of \$3,000 or more, if the amount is received from a financial entity or public body or from a person who is acting on behalf of a client that is a financial entity or public body.
- Re-identify and re-identify the existence of an entity if you previously did so using the methods specified in the AML/ATF legislation in place at the time and kept the associated records, so long as you have no doubts about the information used.
- Verify a corporation's identity again unless you have doubts about the information that was used for that purpose.⁵⁵⁹ Successful client identification need not be repeated for subsequent transactions if the accountant or accounting firm recognizes the client.
- Verify the names of a corporation's directors when you verify the existence of a corporation that is a securities dealer.

⁵⁵⁹ PCMLTFR subsection 155(2)

- Identify an individual or verify the identity and existence of an entity for the receipt of funds in an amount of \$3,000 or more, if the amount is received from a financial entity or public body.
- Identify the individual who conducts a large cash transaction if the cash is received from a financial entity or public body.
- Identify an entity of a group plan account held within a dividend reinvestment plan or a distribution reinvestment plan, including a plan that permits purchases of additional shares or units by the member with contributions other than the dividends or distributions paid by the sponsor of the plan, if the sponsor of the plan is an entity whose shares or units are traded on a Canadian stock exchange, and that operates in a country that is a member of the Financial Action Task Force.

You are not subject to the AML/ATF legislation as an accountant or accounting firm if the activities you undertake are in respect of an audit, review or compilation engagement, or carried out in accordance with the recommendations set out in the *CPA Canada Handbook*.

CHAPTER 25

Appendix K – Obtaining and recording beneficial ownership information

The AML/ATF legislation requires you to obtain, at the time the entity's identity is verified, different information depending on whether you are a corporation or an entity other than a corporation. You must take reasonable measures to confirm the accuracy of the information when it is first obtained.⁵⁶⁰ In all cases (except for not-for-profit organizations), you must collect information establishing the ownership, control and structure of the entity.⁵⁶¹

If you are unable to obtain beneficial ownership information, to keep it up to date in the course of ongoing monitoring of business relationships or to confirm its accuracy,⁵⁶² you must take:

- a. reasonable measures to verify the identity of the entity's chief executive officer or the person who performs that function
- b. the special measures referred to in section 157 of the PCMLTFR

⁵⁶⁰ PCMLTFR subsection 138(2)

⁵⁶¹ PCMLTFR paragraph 138(1)(d)

⁵⁶² PCMLTFR subsection 138(4)

25.1. Beneficial ownership information for a corporation

In the case of a corporation, you must obtain the names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation, and information establishing the ownership, control and structure of the entity.⁵⁶³

You may use the form in Section 25.7 of this guide as an example of a record when obtaining beneficial ownership information.

25.2 Beneficial ownership information for a widely held or publicly traded trust

In the case of a widely held or publicly traded trust, you must obtain the names of all trustees of the trust and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust and information establishing the ownership, control and structure of the entity.⁵⁶⁴

You may use the form in Section 25.7 of this guide as an example of a record when obtaining beneficial ownership information.

25.3 Beneficial ownership information for a trust

In the case of a trust, you must obtain the names and addresses of all trustees and all known beneficiaries and settlors of the trust.⁵⁶⁵

You may use the form in Section 25.7 of this guide as an example of a record when obtaining beneficial ownership information.

25.4 Beneficial ownership information for an entity other than a corporation or trust

In the case of an entity other than a corporation or trust, you must obtain the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity⁵⁶⁶ and information establishing the ownership, control and structure of the entity.

⁵⁶³ PCMLTFR paragraphs 138(1)(a) and (d)

⁵⁶⁴ PCMLTFR paragraphs 138(1)(a.1) and (d)

⁵⁶⁵ PCMLTFR paragraph 138(1)(b)

⁵⁶⁶ PCMLTFR paragraphs 138(1)(c) and (d)

You may use the form in Section 25.7 of this guide as an example of a record when obtaining beneficial ownership information.

25.5 Beneficial ownership for a not-for-profit organization

In the case of a not-for-profit organization, you must keep a record that sets out, whether that entity is (a) a charity registered with the CRA under the Income Tax Act; or (b) an organization, other than one referred to in paragraph (a), that solicits charitable donations from the public.

You may use the form in Section 25.7 of this guide as an example to record this information.⁵⁶⁷

25.6 Record keeping of beneficial ownership information

You must take reasonable measures to confirm the accuracy of the beneficial ownership information when it is first obtained and in the course of ongoing monitoring of business relationships.⁵⁶⁸

See table 29 below. You must keep a record that:

- Sets out the information and the measures taken to confirm the accuracy of the information. If you are not able to obtain the information, to keep it up to date in the course of ongoing monitoring of business relationships or to confirm its accuracy, you must take
 - reasonable measures to verify the identity of the entity's chief executive officer or the person who performs that function
 - the special measures (see further) referred to in section 157 of the PCMLTFR.⁵⁶⁹

⁵⁶⁷ PCMLTFR subsection 138(5)

⁵⁶⁸ PCMLTFR paragraph 123.1(b) and subsection 138(2)

⁵⁶⁹ PCMLTFR section 157: The prescribed special measures that are required to be taken by a person or entity referred to in subsection 9.6(1) of the Act for the purposes of subsection 9.6(3) of the Act are the development and application of written policies and procedures for (a) taking enhanced measures, based on an assessment of the risk, to verify the identity of any person or entity; and (b) taking any other enhanced measure to mitigate the risks, including (i) ensuring, at a frequency appropriate to the level of risk, that client identification information and information collected under section 138 is up to date, and (ii) conducting, at a frequency appropriate to the level of risk, the ongoing monitoring of business relationships referred to in section 123.1.

Special measures referred to in section 157 of the PCMLTFR. FINTRAC has provided examples of special measures to take when dealing with a client that has been identified as high risk.⁵⁷⁰ The non-exhaustive list includes the following:

- taking enhanced measures to verify the identity of persons and entities and verify the existence of entities when they are assessed as high-risk clients
- taking enhanced measures to keep client information up to date
- taking enhanced measures to keep beneficial ownership information up to date
- taking enhanced measures to conduct ongoing monitoring of business relationships for the purposes of detecting transactions that are required to be reported under section 7 of the PCMLTFA (i.e., suspicious transaction reports)
- taking any other enhanced measures to mitigate the risks identified

Accountants and accounting firms are required to keep records for a period of at least five years after the day on which they were created.⁵⁷¹ If a record is the property of a person's employer or of a person or entity with whom they have a contractual relationship, the person is not required to keep the record after the end of their employment or the contractual relationship.

Every required record must be kept in such a way that it can be provided to an authorized person within 30 days after the day on which a request is made to examine it.⁵⁷² Records required to be kept or a copy of the records may be kept in a machine-readable or electronic form if a paper copy can readily be produced from it.

You may use the form in Section 25.7 of this guide as an example of a record when obtaining beneficial ownership information.

⁵⁷⁰ FINTRAC, *Compliance program requirements*, August 4, 2021

⁵⁷¹ PCMLTFR subsection 148(1)

⁵⁷² PCMLTFR section 149

Table 28

Entity type	Information to collect and record	
Corporation	Names of all directors of the corporation and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the shares of the corporation	Information establishing the ownership, control and structure of the entity
Widely held or publicly traded trust	Names of all trustees of the trust and the names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust	
Trust	Names and addresses of all trustees and all known beneficiaries and settlors of the trust	
Entity other than a corporation or trust	The names and addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity	
Not-for-profit organization	<p>Determine if it is a charity registered with the CRA under the Income Tax Act, or</p> <p>An organization, other than a charity registered with the CRA under the Income Tax Act, that solicits charitable donations from the public.</p>	

25.7 Sample – Record of beneficial ownership

Table 29

Sample – Record of beneficial ownership		
Name of corporation	Address	Contact information
ABC Corporation	123 Elm. St, Anywhere, Postal Code	John Doe (000)-555-1212
Name of all directors		
Alex Smith; Brenda Jones; etc.	(Address not mandatory for Directors)	
Names of persons who own or control, directly or indirectly 25 per cent or more of the shares of the corporation (beneficial owners)	per cent shares	Addresses of the beneficial owners* (No P.O. Box numbers)
Dorothy Doe, etc.		999 Oak St., Anywhere, Postal Code

Sample – Record of beneficial ownership			
Name of widely held or publicly traded trust	Names of all trustees of the trust and the names of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust	per cent of units	Contact information - Addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the units of the trust
ABC Trust			
Trustees	Adam Smith		
Owners/controllers	Aretha Doe	X per cent	456 Peel, St. Anywhere, Postal Code: (000)-555-3434
Trust	Names of all trustees and all known beneficiaries and settlors of the trust	Contact information - Addresses of all trustees and all known beneficiaries and settlors of the trust	
Name of trustees	Adam Smith	123 Elm, St, Anywhere, Postal Code: (000)-555-1212	
Name of known beneficiaries	Julie Doe	678 Plum, St, Anywhere, Postal Code: (000)-555-7890	
Name of settlors	Harvey Doe	123 Lake, St, Anywhere, Postal Code: (000)-555-9876	
Name of entity other than a corporation	Names of all persons who own or control, directly or indirectly, 25 per cent or more of the entity	Ownership/control of 25 per cent or more	Contact information - Addresses of all persons who own or control, directly or indirectly, 25 per cent or more of the entity
CBA Partnership	Martin Someone	X per cent	123 Elm. St, Anywhere, Postal Code (000)-555-1212
Not-for-profit organization			
Name of organization		Organization XYZ	
<input type="checkbox"/> Charity registered with the CRA under the Income Tax Act		<input type="checkbox"/> Organization, that is not a Charity registered with the CRA under the Income Tax Act, that solicits charitable donations from the public.	
Description of ownership, control and structure of the entity (not required for not-for-profit organizations)			

CHAPTER 26

Appendix L – Business relationship and ongoing monitoring

Accountants and accounting firms enter into a business relationship with a client the second time that they are required to verify the identity of the client.⁵⁷³ This occurs when there is a:

- receipt of funds of \$3,000 or above
- large cash transaction
- large virtual currency transaction
- suspicious transaction (reasonable measures without tipping off)
- terrorist property involved in the transaction (reasonable measures)

The AML/ATF legislation requires that when you enter into a business relationship with a client you must periodically conduct, based on a risk assessment,⁵⁷⁴ ongoing monitoring of that business relationship for the purpose of:⁵⁷⁵

- detecting a suspicious or attempted suspicious transaction or a terrorist activity financing transaction or attempted terrorist activity financing transaction that must be reported
- keeping client identification information, beneficial ownership⁵⁷⁶ and business relationship⁵⁷⁷ information up to date
- reassessing the level of risk associated with the client's transactions and activities

⁵⁷³ PCMLTFR paragraph 4.1(b)

⁵⁷⁴ PCMLTFA subsection 9.6(2). The risk assessment must be undertaken as per undertaken in accordance with PCMLTFR paragraph 156(1)(c)

⁵⁷⁵ PCMLTFR subsection 123.1

⁵⁷⁶ PCMLTFR section 138

⁵⁷⁷ PCMLTFR section 145

- determining whether transactions or activities are consistent with the information obtained about their client, including the risk assessment of the client

You must also take reasonable measures to confirm the accuracy of the information in the course of ongoing monitoring of business relationships.

26.1 Record keeping

When engaged in a business relationship, accountants and accounting firms must keep a record:

1. that sets out the purpose and intended nature of the business relationship
2. The measures taken:
 - a. the measures taken when you conduct ongoing monitoring of the business relationship, and
 - b. the information obtained from that ongoing monitoring

You are required to keep records for a period of at least five years after the day on which they were created.⁵⁷⁸

If a record is the property of a person's employer or of a person or entity with whom they have a contractual relationship, the person is not required to keep the record after the end of their employment or the contractual relationship.

Every required record must be kept in such a way that it can be provided to an authorized person within 30 days after the day on which a request is made to examine it.⁵⁷⁹ Records required to be kept or a copy of the records may be kept in a machine-readable or electronic form if a paper copy can readily be produced from it.

⁵⁷⁸ PCMLTFR subsection 148(1)
⁵⁷⁹ PCMLTFR section 149

26.1.2 Sample – Record of business relationship information

Table 30

Sample – Record of business relationship information		
Name of entity	Address	Contact information
ABC Corporation	123 Elm. St, Anywhere, Postal Code	John Doe (000)-555-1212
<p>Description of the nature and purpose of business relationship (when second time required to verify the client’s identity):</p> <p>Examples: Transferring funds or securities; paying or receiving funds on behalf of client or purchasing or selling entities or business assets.⁵⁸⁰</p> <p>The corporation wants the accountant or accounting firm to be used for x purpose and expects transactions of y \$ value to be done at frequency z.</p>		
Record the measures taken when you conduct ongoing monitoring of the business relationship with that person or entity and of the information obtained from that ongoing monitoring (PCMLTFR 146(1))		
Date	Rationale for obtaining BRI	Description of reasonable measures taken
June 3, 2021	E.g., first time identifying client	Received \$5,000 in funds for triggering activity.
September 15, 2021	E.g., second time verifying client ID – now have business relationship	Received \$6,000 for another triggering activity. Client assessed as low risk. Business relationship established. The corporation wants the accountant or accounting firm to be used for x purpose and expects transactions of y \$ value to be done at frequency z. Reasonable measures to confirm the accuracy of the information will be applied in the course of ongoing monitoring of the business relationship.

580 FINTRAC, *Business relationship requirements*, Annex 1, August 4, 2021

Sample – Record of business relationship information

January 15, 2022	Ongoing monitoring of business relationship	Because of change in transaction pattern, we determined that the transactions or activities are not consistent with the information obtained about the client, including the risk assessment of the client as low. Client now re-assessed as high risk for the following reason: xyz. Will apply additional enhanced measures abc. We have reassessed the level of risk associated with the client's transactions and activities; we will continue monitoring the business relationship to detect suspicious or attempted suspicious transactions or a terrorist activity financing transactions or attempted terrorist activity financing transactions to be reported; we will keep client identification information, beneficial ownership and business relationship information up to date; and determine whether transactions or activities are consistent with the information obtained about our client, including the risk assessment of the client. We expect the next transaction to occur mid-April. We have scheduled the next business relationship monitoring for mid-April or at the time of the client's next transaction, whichever occurs the earliest.
January 22, 2022	Special (enhanced) measures	Enhanced measures abc applied.
April 22, 2022	Ongoing monitoring of business relationship and special measures	Received \$11,000 in cash from client for triggering activity. LCTR submitted and copy retained. Ongoing monitoring results: (Add all relevant information obtained from the ongoing monitoring).

CHAPTER 27

Appendix M – Large cash transaction report form

27.1 LCTR form, FINTRAC

This form is available at <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/LCTR-eng.pdf> or can be found on FINTRAC's Reporting Forms website at <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng>.

27.2 Completion of the LCTR form

Accountants and accounting firms should refer to the following links for completion and submission of the LCTR form:

- electronically⁵⁸¹
- paper⁵⁸²

581 FINTRAC, *Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically*, February 10, 2022
582 FINTRAC, *Guideline 7B: Submitting Large Cash Transaction Reports to FINTRAC by Paper*, February 10, 2022

CHAPTER 28

Appendix N - Large virtual currency transaction report form

28.1 LVCTR form, FINTRAC

This form is available at: <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/lvctr/LVCTR-eng.pdf> or can be found on FINTRAC's Reporting Forms website at: <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng>

28.2 Field instructions to complete a large virtual currency transaction report

Instructions on how to complete the LVCTR form electronically or on paper can be found at Annex 1 at this website: <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng>

CHAPTER 29

Appendix O – Terrorist property report form

29.1 TPR form, FINTRAC

This form is available at <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/TPR-eng.pdf> or can be found on FINTRAC's Reporting Forms website at <https://www.fintrac-canafe.gc.ca/reporting-declaration/form/form-eng>.

General information on the TPR can be found on FINTRAC's website.⁵⁸³

Please note that at the time of publishing, the TPR form can only be submitted by mail or by fax.

⁵⁸³ FINTRAC, *Reporting terrorist property to FINTRAC*, November 19, 2021

CHAPTER 30

Appendix P – Money laundering and terrorist financing indicators – Accountants

FINTRAC guidance on money laundering and terrorist financing indicators - accountants.⁵⁸⁴

January 2019

This guidance on suspicious transactions is applicable to accountants and accounting firms that are subject to the PCMLTFA and associated regulations. It is recommended that this guidance be read in conjunction with other suspicious transaction report (STR) guidance, including:

- What is a suspicious transaction?
- Reporting suspicious transactions to FINTRAC

This guidance provides money laundering (ML) and terrorist financing (TF) indicators organized by topic:

- ML/TF indicators related to identifying the person or entity
- ML/TF indicators related to client behaviour
- ML/TF indicators surrounding the financial transactions in relation to the person/entity profile
- ML/TF indicators related to products and services
- ML/TF indicators related to change in account activity
- ML/TF indicators based on atypical transactional activity

⁵⁸⁴ Please refer to [FINTRAC's website](#) for any updates. Slight modifications have been made to FINTRAC's text in this Chapter. The official content that can be found on FINTRAC's website. The materials here may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

- ML/TF indicators related to transactions structured below the reporting or identification requirements
- ML/TF indicators involving wire transfers (including electronic funds transfers)
- ML/TF indicators related to transactions that involve non-Canadian jurisdictions
- ML/TF indicators related to use of other parties
- indicators specifically related to terrorist financing
- ML/TF indicators specific to accountants

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours, patterns or other contextual factors that identify irregularities related to financial transactions. These often present inconsistencies with what is expected of your client⁵⁸⁵ based on what you know about them.

The ML/TF indicators in this guidance were developed by FINTRAC through a three-year review of ML/TF cases, a review of high quality STRs, published literature by international organizations such as the Financial Action Task Force (FATF) and the Egmont Group, and consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation but were developed to provide you with a general understanding of what is or could be unusual or suspicious. On its own, a single ML/TF indicator may not appear suspicious. However, observing (an) ML/TF indicator(s) could lead you to conduct an assessment of the transaction(s) to determine whether there are further facts,⁵⁸⁶ contextual elements or additional ML/TF indicators that require the submission of an STR.

Criminal organizations often combine various methods in different ways in order to avoid the detection of ML/TF. If you detect unusual or suspicious behaviour or a transaction that prompts the need for an assessment, ML/TF indicators combined with facts and context⁵⁸⁷ can help you determine if there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators may also be used to explain or articulate the rationale for your reasonable grounds to suspect in the narrative portion of an STR, as they provide valuable information from a financial intelligence perspective.

585 FINTRAC, *Guidance Glossary*, May 4, 2021

586 FINTRAC, *Guidance Glossary*, May 4, 2021

587 FINTRAC, *Guidance Glossary*, May 4, 2021

Important considerations

One piece of the puzzle

The ML/TF indicators in this guidance are not an exhaustive list of ML/TF indicators to support all suspicious scenarios. These ML/TF indicators should be considered as examples to guide the development of your own process to determine when you have reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators are one piece of the puzzle and are designed to complement your own STR program and can be used in conjunction with other publicly available ML/TF indicators.

During an assessment, FINTRAC will review your policies and procedures to see how you use ML/TF indicators within your STR program. Part of the assessment will include evaluating how the actual policies follow your documented approach and determining its effectiveness with respect to the use of ML/TF indicators. This can include a review of transactions to determine how your STR program identifies potential STRs and assesses them using facts, context and ML/TF indicators. For example, you can receive questions if you have not reported an STR for a client you have assessed as high risk and that client activity also matches against multiple ML/TF indicators.

Combination of facts, context and ML/TF indicators

If the context surrounding a transaction is suspicious, it could lead you to assess a client's financial transactions. Facts, context and ML/TF indicators need to be assessed to determine whether there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. On its own, a single financial transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the associated individual or their actions may help you reach the reasonable grounds to suspect threshold.

Alert or triggering system

FINTRAC acknowledges that a reporting entity may have developed a system that relies on specific alerts or triggering events to signal when to assess a transaction to determine if an STR should be submitted to FINTRAC. If you rely on such a system, FINTRAC expects that you review the alerts in a timely manner in order to determine if an STR should be submitted. Regardless of how you choose to operationalize these ML/TF indicators, FINTRAC expects that you will be able to demonstrate that you have an effective process to identify, assess and submit STRs to FINTRAC.

General ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected money laundering and/or terrorist financing. The ability to detect, prevent and deter money laundering and/or terrorist financing begins with properly identifying the person or entity in order to review and report suspicious financial activity.

As an accountant, you may observe these ML/TF indicators over the course of your business activities with a client. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

ML/TF indicators related to identifying the person or entity

The following are examples of ML/TF indicators that you may observe when identifying persons or entities:

- There is an inability to properly identify the client or there are questions surrounding the client's identity.
- The client refuses or tries to avoid providing information required, or provides information that is misleading, vague or difficult to verify.
- The client refuses to provide information regarding beneficial owners or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification presented by the client cannot be verified (e.g., it is a copy).
- There are inconsistencies in the identification documents or different identifiers provided by the client, such as address, date of birth or phone number.
- Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Client displays a pattern of name variations from one transaction to another or uses aliases.
- Client alters the transaction after being asked for identity documents.
- The client provides only a non-civic address such as a post office box or disguises a post office box as a civic address for the purpose of concealing their physical residence.
- Common identifiers (e.g., addresses, phone numbers, etc.) used by multiple clients that do not appear to be related.
- Common identifiers (e.g., addresses, phone numbers, etc.) used by multiple clients conducting similar transactions.
- Transactions involve individual(s) or entity(ies) identified by media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client are difficult.

ML/TF indicators related to client behaviour

The contextual information acquired through the “know your client”⁵⁸⁸ requirements or the behaviour of a client, particularly surrounding a transaction or a pattern of transactions, may lead you to conduct an assessment in order to determine if you are required to submit an STR to FINTRAC. The following are some examples of ML/TF indicators that are linked to contextual behaviour and may be used in conjunction with your assessment and your risk-based approach:

- The client makes statements about involvement in criminal activities.
- There is evidence of untruthfulness on behalf of the client (e.g., providing false or misleading information).
- The client exhibits nervous behaviour.
- The client refuses to provide information when required or is reluctant to provide information.
- The client has a defensive stance to questioning.
- The client presents confusing details about the transaction or knows few details about its purpose.
- The client avoids contact with reporting entity employees.
- The client refuses to identify a source for funds or provides information that is false, misleading or substantially incorrect.
- The client exhibits a lack of concern about higher-than-normal transaction costs or fees.
- The client makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- There is insufficient explanation for source of funds.

ML/TF indicators surrounding the financial transactions in relation to the person/entity profile

Clearly understanding the expected activity of a person or entity will allow you to assess their financial activity with the proper lens. For example, an entity involved in an industry that is not normally cash intensive receiving excessive cash deposits or a person conducting financial transactions atypical of their financial profile. The following are some examples of ML/TF indicators surrounding the financial transactions related to person/entity profile:

- The transactional activity far exceeds the projected activity at the beginning of the relationship.
- The transactional activity (level or volume) is inconsistent with the client’s apparent financial standing, their usual pattern of activities or occupational information (e.g., student, unemployed, social assistance, etc.).

⁵⁸⁸ FINTRAC, *Know your client requirements*, June 1, 2021

- The transactional activity is inconsistent with what is expected from a declared business (e.g., business account has no normal business-related activities, such as the payment of payrolls or invoices).
- The client appears to be living beyond their means.
- Large and/or rapid movement of funds is not commensurate with the client's financial profile.
- Rounded sum transactions that are atypical of what would be expected from the client.
- Size or type of transactions that are atypical of what is expected from the client.
- The client's address or employment address is outside the local service area without a reasonable explanation.
- There is a sudden change in the client's financial profile, pattern of activity or transactions.
- The client uses notes, monetary instruments, or products and/or services that are unusual for such a client.

ML/TF indicators related to products and services

Accounts can take different forms (e.g., chequing, savings, investment, etc.) and for the purposes of this section, the ML/TF indicators below will aim to address the ML/TF risks linked to different types of accounts held by various reporting entities in Canada. There are many ML/TF indicators related to account activity. Your process to evaluate risk for products and services you provide should be documented as part of your “know your client” and risk-based approach⁵⁸⁹ requirements. The following ML/TF indicators will focus on products or services that may be applicable within your business:

- holding multiple accounts at several financial institutions for no apparent reason⁵⁹⁰
- suspected use of a personal account for business purposes, or vice-versa
- the client appearing to have recently established a series of new relationships with different financial entities
- a product and/or service opened on behalf of a person or entity that is inconsistent based on what you know about that client
- accounts used for pass-through activities (e.g., to receive and subsequently send funds to beneficiaries)
- use of multiple foreign bank accounts for no apparent reason
- frequent and/or atypical transfers between the client's products and accounts for no apparent reason
- the same individual(s) holding signing authority for accounts held by multiple entities where there is no legal reason or sufficient explanation for such an arrangement
- accounts held by multiple entities either headquartered at the same location or having the same directors/signing authorities for no apparent reason

⁵⁸⁹ FINTRAC, *Risk assessment guidance*, August 4, 2021
⁵⁹⁰ FINTRAC, *Guidance Glossary*, May 4, 2021

ML/TF indicators related to change in account activity

Certain changes regarding an account may be indicative of ML/TF for a multitude of reasons including, but not limited to, the use of an account to suddenly launder or transmit funds, an increase in volume, changes in ownership of an account, etc. Changes in account activity may trigger a need for further assessment of the person or entity holding the account and some examples to consider are listed below:

- A business account has a change in ownership structure with increases in transactional activity and no apparent explanation.
- An inactive account begins to see financial activity (e.g., deposits, wire transfers, withdrawals).
- Accounts that receive relevant periodical deposits and are inactive at other periods without a logical explanation.
- There is an abrupt change in account activity.

ML/TF indicators based on a typical transactional activity

There are certain transactions that are outside the normal conduct of your everyday business. These transactions may be indicative of a suspicious transaction and would require additional assessment. Some examples of ML/TF indicators based on atypical transactional activity are listed below:

- The client has multiple products at the same institution, atypical of what would be expected.
- There is a series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- Transactions display financial connections between individuals or businesses that are not usually connected (e.g., a food importer dealing with an automobile parts exporter).
- Transaction is unnecessarily complex for its stated purpose.
- The client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- The client's transactions have no apparent business or economic purpose.
- Transaction is consistent with publicly known trends in criminal activity.
- The client presents musty, odd smelling or extremely dirty bills.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).
- There are atypical transfers by client on an in-and-out basis, or other methods of moving funds quickly, such as a cash deposit followed immediately by a wire transfer of the funds out.
- Funds are transferred in and out of an account on the same day or within a relatively short period of time.

ML/TF indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML/TF offence. There are multiple thresholds which trigger reporting/identification requirements by a reporting entity. Some examples of ML/TF indicators which may be indicative of a person or entity attempting to evade identification and/or reporting thresholds are listed below:

- The client appears to be structuring amounts to avoid client identification or reporting thresholds.
- The client appears to be collaborating with others to avoid client identification or reporting thresholds.
- Multiple transactions are conducted below the reporting threshold within a short time period.
- The client makes inquiries that would indicate a desire to avoid reporting.
- The client exhibits knowledge of reporting thresholds.

ML/TF indicators involving wire transfers (including electronic funds transfers)

In our current global environment, it is increasingly easier to transfer funds to, from or through multiple jurisdictions (municipal, national or international) in a rapid fashion. This presents an increased ML/TF risk as transactions through multiple accounts and/or jurisdictions increases the difficulty for reporting entities and law enforcement to trace illicit funds. Examples of these types of transactions which may require further assessment include the following:

- The client is unaware of details surrounding incoming wire transfers, such as the ordering client details, amounts or reasons.
- The client does not appear to know the sender of the wire transfer from whom the wire transfer was received, or the recipient to whom they are sending the wire transfer.
- The client requests wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond to the expected use of the account type or business account.
- The client is accompanied by individuals who appear to be sending or receiving wire transfers on their behalf.
- The client attempts to specify the routing of an international wire transfer.
- The client utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.
- Funds are deposited or received into several accounts and then consolidated into one before transferring the funds outside the country.
- Immediately after transferred funds have cleared, the client moves funds to another account or to another individual or entity.

- Multiple clients have sent wire transfers over a short period of time to the same recipient.
- A large wire transfer or a high volume of wire transfers are conducted or received through the account that do(es) not fit the expected pattern of that account.
- Large and/or frequent wire transfers occur between senders and receivers with no apparent relationship.
- The client sends to, or receives wire transfers from, multiple clients.

ML/TF indicators related to transactions that involve non-Canadian jurisdictions

There are certain types of transactions that may be sent or received from jurisdictions outside of Canada where there is higher ML/TF risk due to more permissible laws or the local ML/TF threat environment. The following are examples to consider when making an assessment of the financial transaction conducted by a person/entity through your business:

- transactions with jurisdictions that are known to produce or transit drugs or precursor chemicals or are sources of other types of criminality
- transactions with jurisdictions that are known to be at a higher risk of ML/TF
- transaction/business activity involving locations of concern, which can include jurisdictions where there are ongoing conflicts (and periphery areas), countries with weak money laundering/terrorist financing controls, or countries with highly secretive banking or other transactional laws such as transfer limits set by a government
- transactions involving any countries deemed high risk or non-cooperative by the FATF
- the client making frequent overseas transfers, not in line with their financial profile

Due to the ever-evolving nature of the ML/TF environment, high risk jurisdictions and trends are often subject to change. To ensure that you are referencing accurate information, FINTRAC encourages you to research publicly available sources on a regular basis to support these ML/TF indicators as part of your STR program. There are multiple sources that identify jurisdictions of concern, including the FATF which publishes contextual information on high-risk jurisdictions in relation to their risk of money laundering and terrorist financing. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorists operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk-based approach and internal STR program.

ML/TF indicators related to use of other parties

In the course of a 'normal' financial transaction, there are a 'normal' number of parties who are engaging in the transaction, depending on the nature of the transaction at hand. For example, in the instance of depositing cash to a personal bank account, there is generally one party to the transaction: the individual who holds the account depositing into their own account. In contrast, with the deposit of cash to a business account, you can have many different roles that may be expected, including individuals associated with the business's finance function holding authority over the account, while another employee may be charged with depositing the cash.

Transactions that involve parties not typically associated with a transaction can present an elevated risk of money laundering and/or terrorist financing. These additional parties can be used to allow a criminal to avoid being identified or being linked to an asset or account. This section includes examples of how the involvement of other parties may be indicative of the structure of a criminal enterprise. Some examples of such other parties include the use of a third-party or nominee.

Use of third-party

A third-party is any individual or entity that instructs someone to act on their behalf for a financial activity or transaction. There are some situations where there is an apparent and discernable rationale for the inclusion of the third-party in a transaction and this may not be suspicious. However, you may become suspicious in a situation where the reason for a third-party acting on behalf of another person or entity does not make sense based on what you know about the client or the third-party. Use of third-parties is one method that money launderers and terrorist financiers use to distance themselves from the proceeds of crime or source of criminally obtained funds. By relying on other parties to conduct transactions they can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Some examples of ML/TF indicators related to the use of a third-party can be found below:

- multiple deposits that are made to an account by non-account holders
- unrelated parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient
- a client conducting a transaction while accompanied, overseen or directed by another party
- a client making numerous outgoing payments to unrelated parties shortly after they receive incoming funds
- wire transfers, deposits or payments to or from unrelated parties (foreign or domestic)
- client appears or states to be acting on behalf of another party
- account that is linked to seemingly unconnected parties

Use of nominee

A nominee is a particular type of other party that is authorized to open accounts and conduct transactions on behalf of a person or entity. There are legitimate reasons for relying on a nominee to conduct financial activity of behalf of someone else.

However, this type of activity is particularly vulnerable to ML/TF as it is a common method used by criminals to distance themselves from the transactions that could be linked to suspected ML/TF offences. These are some examples of ML/TF indicators relating to the misuse of nominees:

- An individual maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- An individual or entity other than the stated account holder conducts the majority of the transaction activity which seems unnecessary or excessive.
- The client is involved in transactions or account activity that are suspicious but refuses or is unable to answer questions related to the account or transactions.

Indicators related to terrorist financing

In Canada, terrorist financing offences make it a crime to knowingly collect or provide property, which can include financial or other related services, for terrorist purposes. This section is focused on examples that are specific to the possible commission of a terrorist financing offence. However, please note that the other ML/TF indicators in this guidance may also prove relevant in determining when you have reasonable grounds to suspect the commission of terrorist financing, as the methods used by criminals to evade detection of money laundering are similar.

Indicators specifically related to terrorist financing:

The indicators below are some examples of indicators relating to terrorist financing:

- transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls
- an account opened in the name of an entity, foundation or association, which may be linked to or involved with a suspected terrorist organization
- the use of funds by a non-profit organization not consistent with the purpose for which it was established
- raising donations in an unofficial or unregistered manner
- client identified by media or law enforcement as having travelled, attempted or intended to travel, to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations
- transactions involve individual(s) or entity(ies) identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities

- law enforcement information provided which indicates individual(s) or entity(ies) may be linked to a terrorist organization or terrorist activities
- client conducted travel-related purchases (e.g., purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations
- individual or entity's online presence supports violent extremism or radicalization
- client donates to a cause that is subject to derogatory information that is publicly available (e.g., crowdfunding initiative, charity, NPO, NGO, etc.)

ML/TF indicators specific to accountants

In addition to the general ML/TF indicators that have been highlighted in this guidance, there may be more specific ML/TF indicators related to your business as an accountant. Below are some examples of sector specific ML/TF indicators that you should consider as part of your STR program:

- The client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- The client has a history of changing bookkeepers or accountants yearly.
- The client is uncertain about location of company records.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- The company has no employees, which is unusual for the type of business.
- The company is paying unusual consultant fees to offshore companies.
- The 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.
- The 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.
- The company makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- The 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.
- The 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.

CHAPTER 31

Appendix Q – Indicators of ML/TF related to virtual currencies

FINTRAC has published a list of indicators of ML/TF related to virtual currencies.⁵⁹¹ These indicators are red flags that were developed to provide reporting entities with a general understanding of what is or could be unusual or suspicious when dealing in virtual currencies.

Virtual currency ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected ML and/or TF. The ability to detect, prevent and deter ML and/or TF begins with properly identifying the person or entity in order to review and report suspicious financial activity. You may observe these ML/TF indicators over the course of your business activities with a client. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

- Client portfolio only consists of privacy coins or has a high value in privacy coins (For example, Monero, Dash, Zcash).
- The client transfers Bitcoin in large volumes in exchange for privacy coins (For example Monero, Dash, Zcash, etc.).
- The client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.
- Virtual currency addresses match addresses on recognized watch lists such as the list of the Office of Foreign Assets Control (OFAC) or law enforcement information.

⁵⁹¹ FINTRAC, *Money laundering and terrorist financing indicators—Virtual currency transactions*, June 1, 2021. This content is a reproduction of the official content that can be found on FINTRAC's website. The materials may be out-of-date. The reproduction has not been produced in affiliation with, or with the endorsement of FINTRAC.

- Many individuals register with the exchange within a short period using a shared address, mobile device, phone number, IP addresses and other common identity indicators.
- The client's virtual currency wallet or address is linked to fraudulent activity in media reports and/or cyber security bulletins.
- A platform receives unusual or persistent requests from other exchanges/vendors/service providers in respect of a client's deposited funds.
- A broker charges abnormally high commission fees compared to the industry standard.
- The white paper is of poor quality, incomplete, misleading and has limited information.⁵⁹²
- Publicity is created around the initial coin offering (ICO) (advertisements, celebrity endorsements, social media ads), also known as pump and dump ICOs.
- The developers are anonymous, or information provided about the ICO cannot be verified.
- There is no access to the smart contract, to the code or to technical information about the token's creation.
- There is no possibility to sell the investment or to exit the project to recover the invested funds.
- A series of complicated transfers of funds to multiple addresses or wallets that seems to be an attempt to hide the source and intended use of the funds.
- Transactions take place at the same time of day.
- Transfers are made from fiat to virtual currency and virtual currency to fiat.
- There is a high volume and frequency of transfers between different types of virtual currencies.
- Client provides an anonymous email address obtained through an encrypted email service.
- Funds are deposited or withdrawn from a virtual currency address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (for example, ransomware) and/or theft reports.
- Funds flow through a large number of intermediate addresses in a very short period of time prior to being deposited in a client's wallet, or just after being withdrawn.
- Virtual currency passes through mixers/tumblers and is transferred to multiple wallets, where the funds are cashed out.
- The virtual currency's funds originated from an over-the-counter trade broker that advertises its services as privacy-oriented/anonymous.

⁵⁹² A white paper in the VC context is a document issued by a new blockchain project before its Initial Coin Offering (ICO), which provides information such as the technology, methodology, product and service being launched.

- Virtual currency address has links or hops from a wallet address that has appeared on online platforms indicating support for violent extremism or radicalization (including social media, ads on fundraising sites, sites on Tor or messaging sites).
- The source of funds used for the purchase of large amounts of virtual currencies is unknown.
- The email address used in the transaction is linked to advertisements for the sale of virtual currencies on peer-to-peer exchange platforms. These advertisements may suggest that the client is buying and selling virtual currency on a commercial scale through a business as a non-registered money services business.
- The client frequently receives funds from multiple payment processors.
- The client makes frequent payments or transfers to companies, post office mailing services or uses money orders from agents of the Crown for the purchase of computer software or hardware.

CHAPTER 32

Appendix R – Third-party determination record when receiving \$10,000 or more in cash or virtual currency

32.1 Requirement

When receiving an amount of \$10,000 or more in cash or in virtual currency, you must keep either a large cash transaction record or a large virtual currency transaction record, or both types of records if you receive \$10,000 or more in each form (cash or virtual currency). You must take, upon receipt, reasonable measures to determine whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party.⁵⁹³

If you determine that the person from whom the cash or virtual currency is received is acting on behalf of a third-party, you must take reasonable measures to obtain the following information and keep a record of the information obtained:⁵⁹⁴

- a. if the third-party is a **person**, their name, address and date of birth and the nature of their principal business or their occupation
- b. if the third-party is an **entity**, its name and address, the nature of its principal business, its registration or incorporation number and the jurisdiction and country of issue of that number

⁵⁹³ PCMLTFR subsection 134(1)
⁵⁹⁴ PCMLTFR subsection 134(2)

- c. the **relationship** between the third-party and the person from whom the cash or virtual currency is received

If you are not able to determine⁵⁹⁵ whether the person from whom the cash or virtual currency is received is acting on behalf of a third-party but there are reasonable grounds to suspect that they are, you must keep a record that:

- a. indicates whether, according to the person from whom the cash or virtual currency is received, they are acting on their own behalf only
- b. describes the reasonable grounds to suspect that they are acting on behalf of a third-party

595 PCMLTFR subsection 134(3)

32.2 Form – Third-party determination record

Table 31

THIRD PARTY DETERMINATION RECORD		
The following information must be collected, retained and recorded for each prescribed transaction where the Accountant or Accounting Firm receives \$10,000 or more in cash or virtual currency from a client in respect of Triggering Activities when determining if a third party is giving instructions to your client or you have reasonable grounds to suspect that they are acting on behalf of a third party.		
INFORMATION ON THE PERSON FROM WHOM YOU RECEIVED THE CAD \$10,000 OR MORE IN CASH OR VIRTUAL CURRENCY		
Last Name		First Name
Street Address		Apartment/Unit #
City	Prov./Terr.	Postal Code
Date of Birth		Nature of Principal Business or Occupation
INFORMATION WHEN AMOUNT IS RECEIVED FROM AN ENTITY		
Name of Entity		Nature of Principal Business
Street Address		Apartment/Unit #
City	Prov./Terr.	Postal Code
Registration or Incorporation Number	Jurisdiction of Issue of Number	Country of Issue of Number
IF YOU CANNOT DETERMINE IF THE PERSON IS ACTING ON BEHALF OF A THIRD PARTY		
If you are not able to determine whether the person from whom the cash or virtual currency is received is acting on behalf of a third party but there are reasonable grounds to suspect that they are, you must keep a record of the following:		
1. According to the person from whom the cash or virtual currency is received, are they are acting on their own behalf only?		
<input type="checkbox"/> YES <input type="checkbox"/> NO		
2. Describe the reasonable grounds to suspect that the person from whom the cash or virtual currency is received is acting on behalf of a third party:		

CHAPTER 33

Appendix S – Self-review checklist

Part A: Compliance framework evaluation

Table 32

Requirements	Status	Comments
Compliance officer		
Has the compliance officer been appointed, in writing, to their role?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is the compliance officer independent of operations?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is the job description of the compliance officer described in writing, in sufficient detail, with documented accountability for the AML/ATF program content and design?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the compliance officer have: <ol style="list-style-type: none"> 1. appropriate qualifications 2. knowledge of regulatory requirements 3. money laundering subject matter expertise and reference to policies 4. adequate resources to achieve program objectives 5. documented unfettered access to senior management, the board, and all information and individuals throughout the organization 	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is there a substitute compliance officer in case of absence by the primary?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Policies and procedures		
Do policies incorporate all the objectives and responsibilities imposed by the legislation, including a risk management mandate?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do procedures address the nature, timing, responsibilities, process and persons involved for all legislative requirements applicable to the organization, including: <ol style="list-style-type: none"> 1. record keeping 2. client identification (personal and non-personal) and prohibitions on accepting or dealing with clients where identification does not occur 3. risk-based approach measures required/mandated by law, and elected by your organization 4. suspicious transaction reporting 5. tipping-off prohibitions 6. large cash transaction report 7. large virtual currency transaction report 8. Ministerial directives and transaction limitations/prohibitions 9. PEPs, HIOs, their family members and close associates 10. obtaining beneficial ownership information 11. compliance program requirements (including risk-based approach (RBA) documentation; the appointment of a compliance officer; the maintenance of up-to-date policies and procedures; the requirement for a bi-annual compliance review; the requirement for ongoing training for all employees and agents); the requirement for a risk assessment taking into account all factors including the development and implementation of new technologies 	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Have the policies and procedures been approved by a senior officer of the organization?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do our policies and procedures describe the processes we follow when using the reliance method to verify the identity of corporations and other entities and how we ensure that the information is valid and current?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do our policies and procedures describe the processes we follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how we ensure that the information is authentic, valid and current?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Do our policies and procedures explain our process for submitting TPRs, including our process to identify terrorist property? Do they include processes to ensure TPRs are complete, accurate and submitted to FINTRAC immediately?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does our training program ensure our employees, agents or other individuals authorized to act on our behalf are aware of our terrorist property reporting requirements?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Risk assessment & risk-based approach		
Has an inherent risk assessment been conducted and does it include the following prescribed factors? 1. clients and business relationships 2. products and delivery channels 3. geographic location of the activities 4. other relevant factors	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Based on the above inherent risk assessment, are all areas classified into respective risk levels?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the risk-based approach (RBA) documentation contain the minimum required components? 1. documented inherent risk assessment 2. risk mitigation strategy	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the documented risk mitigation strategy address all higher risk areas identified in the inherent risk assessment to a level acceptable by the organization, with at least the minimum standards imposed by the legislation (ongoing monitoring and client identification updates)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are risk mitigation measures integrated into policies and procedures?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Have the relevant employees been trained appropriately in the reason and application of risk mitigation measures?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are policies and procedures adopted for risk mitigation strategies being followed?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are risks being managed within organizational tolerance levels (are controls meeting their objective/resulting in the expected outcome)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are resource allocations appropriate given inherent risk assessment findings and risk mitigation experience?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Training		
Does the organization have a documented training program which specifies: 1. Who is to be trained? 2. With what frequency will the training occur to satisfy the ongoing nature of the program? 3. How will the content be used for training? 4. What restrictions, if any, will be placed on staff prior to successfully completing the training? 5. How will content retention be evaluated and documented? 6. On what basis will employees and agents be exempted from training?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the training content include at least: 1. background on money laundering risks 2. AML/ATF requirements including identifying reportable transactions 3. consequences of non-compliance and potential fines/penalties 4. organizational policies and procedures	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are there enhanced training requirements for the compliance officer?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Effectiveness review		
Has an effectiveness review been conducted within two years of the previous review?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is the effectiveness review conducted by a person or firm independent of the organization's operations?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is the effectiveness review conducted by a person or firm with expertise in the AML/ATF legislation, money laundering risks and an understanding of the organization's operations?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the effectiveness review document specify a definition for effectiveness, the standards against which it evaluates effectiveness, its scope, methodology, findings, recommendations and management undertakings to the recommendations?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Has the effectiveness review evaluated the effectiveness of: 1. policies and procedures (conformance to relevant standards and operational adherence) 2. the risk assessment and risk-based approach 3. the risk mitigation program 4. training	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Has the effectiveness review report been presented to a senior officer within 30 days after the assessment along with any updates, if applicable, made to policies and procedures within the reporting period and the status of implementing any changes, if applicable, to policies and procedures?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Part B: Operational compliance evaluation

Table 33

Requirements	Status	Comments
Client identification		
Are legislative and internal standards being adhered to for the acceptance of personal clients (e.g., valid identification with details recorded)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are legislative and internal standards being adhered to for the acceptance of business clients (e.g., timing, extent of documentation)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are legislative and internal standards being adhered to for the acceptance of not-for-profit clients?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are enhanced identification processes being followed for higher risk clients?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are identity verification standards being adhered to in cases where the client or their signing authority is not physically present when identifying themselves?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is client information being updated for higher risk clients?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Is third-party determination conducted and documented in the required circumstances?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Large cash/Large virtual currency transaction report (LCTR/LVCTR)		
Does the organization have an effective system in place to detect individual transactions, and combinations of transactions (24-hour rule) which require reporting?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are all reportable transactions reported within the prescribed timeframe and with all the required details (timing and quality of reporting)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
In reference to the 24-hour rule, do our policies and procedures include the time when our 24-hour windows begin and end? And do we indicate the times that our 24-hour window begins and ends in a mandatory field when we submit a report to FINTRAC?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Suspicious and attempted suspicious transaction reporting (STR)		
Does the organization have effective systems and training in place for the detection of transactions, attempted transactions and combinations of transactions which require reporting?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the organization have an effective system in place to evaluate and document unusual transactions, whether attempted or completed, put forward by employees and technology?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are submitted STRs consistent in the detection, assessment and submission of STRs? If certain ML/TF indicators are supporting our suspicions of ML/TF, do these indicators apply to other situations to ensure that we are not missing suspicious transactions that should be or should have been reported to FINTRAC?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
If an STR was submitted to FINTRAC in respect of a transaction conducted by an individual or entity, have we continued to submit reports on the client's transactions as long as they remain suspicious?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do we work with others in our business sector to learn how others are detecting, assessing and reaching RGS the commission of ML/TF and to establish common ideas of what could be considered unusual or suspicious?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do we review the measures taken to identify the relevant information in the STRs (facts, context and ML/TF indicators) and when this information became known to ensure that we are reporting as soon as practicable from the date we reached the RGS threshold?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Do we consider the consistency and integrity of our "know your client" information and provide all relevant information to FINTRAC that leads to our determination of the RGS threshold being met?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Is the rationale from the evaluation of unusual transactions fully documented? For both reported suspicious transactions and unreported transactions not deemed to be suspicious?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are all reportable transactions reported within the prescribed timeframe and with all the required details (timing and quality of reporting)?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Have reasonable measures been taken to determine the identification of the subjects within all STRs?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Have suspicious and attempted suspicious transactions been linked to risk assessment and risk mitigation measures?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Terrorist property reporting (TPR)		
Does the organization have effective systems and training in place for the detection of transactions and property which require reporting?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Does the organization have an effective system in place to evaluate and document potentially reportable transactions and property?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
Are all reportable transactions and properties reported to FINTRAC, CSIS and the RCMP within the prescribed timeframe and with all the required details?	YES <input type="checkbox"/> NO <input type="checkbox"/>	

Requirements	Status	Comments
Record keeping and retention		
Are the prescribed records retained for a period of at least five years, in a way that allows for their retrieval within 30 days of a request by FINTRAC?	YES <input type="checkbox"/> NO <input type="checkbox"/>	
<p>Are sufficient details kept about the following transactions and situations at the prescribed thresholds:</p> <ol style="list-style-type: none"> 1. receipt of funds record 2. record of verification of the identity of the client (for large cash transactions, large virtual currency transactions, suspicious transactions and terrorist property reports) 3. business relationship record 4. ongoing business relationship record 5. record of reasonable measures to confirm the accuracy of beneficial ownership information 6. copy of large cash transaction report 7. large cash transaction record 8. record of reasonable measures taken determining the third-party in a large cash or large virtual currency transaction 9. record of grounds to suspect third-party involvement in a large cash/large virtual currency transaction 10. copy of large virtual currency transaction report 11. large virtual currency transaction record 12. copy of the suspicious transaction or attempted transaction report 13. copy of the terrorist property report 14. record of PEP, HIO, family and close associate when receiving \$100,000 or more in cash or virtual currency 15. record of PEP, HIO, family and close associate when a business relationship is or may be involved 	YES <input type="checkbox"/> NO <input type="checkbox"/>	



CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
CPACANADA.CA