



Government
of Canada

Gouvernement
du Canada

[Canada.ca](#) › [FINTRAC](#) › [Obligations and guidance](#) › [Penalties for non-compliance](#)

Guide on harm done assessment for "Know your client" requirements violations

On this page

1. [Introduction](#)

1.1 [Purpose of the guide](#)

1.2 [Definition of harm](#)

1.3 [Considering harm in AMP calculations](#)

2. [Violations related to "Know your client" \(KYC\) requirements](#)

3. [Violation related to opening an account when client identity cannot be established](#)

3.1 [Harm done in the case of a violation related to opening an account when client identity cannot be established](#)

3.2 [Penalty determination for a violation related to opening an account when client identity cannot be established](#)

4. [Violations related to verifying client identity](#)

4.1 [Harm done in the case of violations related to verifying client identity](#)

4.2 Penalty determination for violations related to verifying client identity.

4.3 Violations related to client identification information records

5. Violations related to third party determination

5.1 Harm done in the case of violations related to third party determination

5.2 Penalty determination for violations related to third party determination

5.3 Violations related to third party information records

6. Violation related to inter vivos trust information records

7. Violation related to beneficial ownership

7.1 Harm done in the case of a violation related to beneficial ownership

7.2 Penalty determination for a violation related to beneficial ownership

8. Violation related to confirming the accuracy of information on the control of an entity.

8.1 Harm done in the case of a violation related to confirming the accuracy of information on the control of an entity.

8.2 Penalty determination for a violation related to confirming the accuracy of information on the control of an entity.

9. Violation related to records on beneficial ownership information

10. Violation related to ascertaining the identity of an entity's most senior managing officer

10.1 Harm done in the case of a violation related to ascertaining the identity of an entity's most senior managing officer

10.2 Penalty determination for a violation related to ascertaining the identity of an entity's most senior managing officer

11. Violations related to politically exposed persons (PEP) and heads of international organizations (HIO) determination

11.1 Harm done in the case of violations related to PEP and HIO determination

11.2 Penalty determination for violations related to PEP and HIO determination

12. Violations related to source of funds determination

12.1 Harm done in the case of violations related to source of funds determination

12.2 Penalty determination for violations related to source of funds determination

13. Violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

13.1 Harm done in the case of violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

13.2 Penalty determination for violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

14. Violations related to records for PEPs and HIOs.

14.1 Violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

14.2 Harm done in the case of a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

- 14.3 Penalty determination for a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account
- 15. Violation related to ongoing monitoring of business relationships
 - 15.1 Harm done in the case of a violation related to ongoing monitoring of business relationships
 - 15.2 Penalty determination for a violation related to ongoing monitoring of business relationships
- 16. Violations related to treating the activities of a person or an entity as high-risk
 - 16.1 Harm done in the case of violations related to treating the activities of a person or an entity as high-risk
 - 16.2 Penalty determination for violations related to treating the activities of a person or an entity as high-risk
- 17. Repeated instances of a given violation

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to "Know your client" violations.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations.

According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other

criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the Act ¹ or with FINTRAC's ability to carry out its mandate ². Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific

violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to "Know your client" (KYC) requirements

One of the most important things we can do to protect our financial system from being exploited for ML/TF activities is to remove anonymity from financial transactions.

Criminals convert, conceal and transfer their assets without detection by hiding their identities when conducting financial transactions.

Therefore, requirements such as verifying the identity of individuals, confirming the existence of entities, determining whether a person is acting on behalf of a third party or if an account will be used by a third party, and determining the beneficial ownership of an entity have been put in place to make our financial system less anonymous. As a consequence of these requirements, those who are conducting transactions, and those that are directly or indirectly in control of, or benefit from funds and transactions, will be known and this information will be documented. These measures are of utmost importance to detect, prevent and deter the exploitation of Canada's financial system. Violations related to these requirements interfere with the achievement of subparagraph 3(a)(i) of the Act and result in vulnerabilities in Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime, particularly when it comes to detecting ML/TF activities and deterring those criminals who would use our financial system for these purposes.

3. Violation related to opening an account when client identity cannot be established

This section outlines FINTRAC's approach to the violation for opening an account for a client when their identity cannot be established, including the harm assessment and penalty calculation.

Table 1—Violation related to opening an account when client identity cannot be established

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.2	53.2 64 65 66	Opening an account for a client by a specified person or entity in the prescribed circumstances when the identity of the client cannot be established in accordance with prescribed measures	Serious \$1-\$100,000

3.1 Harm done in the case of a violation related to opening an account when client identity cannot be established

If an account is knowingly opened but the identity of the account holder cannot be verified, then the account holder can control the funds without being directly associated to the funds, and without being detected. Anonymous financial transactions and activities allow criminals to accumulate, transfer, convert and conceal assets from the authorities. In order to protect Canada's financial system from abuse, financial entities, securities dealers and casinos are prohibited from opening an account for a client whose identity cannot be ascertained.

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind the transactions. This requirement deters those who would launder the proceeds of crime or finance terrorist activities, and when combined with record keeping requirements, it also serves as a tool for law enforcement to investigate and prosecute ML/TF-related offences.

3.2 Penalty determination for a violation related to opening an account when client identity cannot be established

When an account has been opened for client and their identity cannot be verified in accordance with the Act and its regulations, and at least one financial transaction has been conducted on the account, the maximum prescribed penalty of \$100,000 is applied. If no transaction has been conducted, FINTRAC may consider this to be a mitigating factor and reduce the penalty.

4. Violations related to verifying client identity

This section outlines FINTRAC's approach to the violations related to the requirement to verify client identity in prescribed circumstances, including the harm assessment and penalty calculation.

Table 2—Violations related to verifying client identity

Provision of the Act	Provision of the PCMLTFR	Description ³	Classification of violation
----------------------	--------------------------	--------------------------	-----------------------------

6.1	53, 64(1) and 64(2) (b);	Failure of a specified person or entity to ascertain in the prescribed manner and within the prescribed period the identity of every individual under the prescribed circumstances	Minor \$1-\$1,000
6.1	53.1, 64(1) and 64(2) (b.1);		
6.1	54(b), 64(1) and 64(2) (b);		
6.1	54(a), 64(1) and 64(2) (a);		
6.1	54.1(a), 64(1) and 64(2)(b.2);		
6.1	55(a), 64(1) and 64(2) (c);		
6.1	55(d)(ii), 64(1) and 64(2)(c);		
6.1	55(e), 64(1) and 64(2) (c);		
6.1	57(1), 64(1) and 64(2) (a);		

6.1	59(1)(a), 64(1) and 64(2)(b);		
6.1	59(1)(b), 64(1) and 64(2)(b);		
6.1	59(1)(c), 64(1) and 64(2)(b);		
6.1	59.1(a), 64(1) and 64(2)(e);		
6.1	59.2(1)(a), 64(1) and 64(2)(e);		
6.1	59.3(a), 64(1) and 64(2)(b);		
6.1	59.5(a), 64(1) and 64(2)(b);		
6.1	60(a), 64(1) and 64(2) (e.1);		
6.1	60(b)(ii), 64(1) and 64(2)(b);		

6.1	60(b)(iii), 64(1) and 64(2)(b);		
6.1	60(b)(iv), 64(1) and 64(2)(b);		
6.1	61(a), 64(1) and 64(2) (d)		
6.1	61(b), 64(1) and 64(2) (b)		

6.1	54.1(b), 65(1) and 65(2)(a.1);	Failure of a specified reporting entity to confirm in the prescribed manner and within the prescribed period the existence of every entity under prescribed circumstances	Minor \$1-\$1,000
6.1	54.1(c), 66(1) and 66(2)(a.1)		
6.1	54(d), 65(1) and 65(2) (a)		
6.1	54(e), 66(1) and 66(2) (a)		
6.1	55(b), 65(1) and 65(2) (b)		
6.1	55(c), 66(1) and 66(2) (b)		
6.1	55(d)(i), 65(1), 65(2) (b) or 55(d) (i), 66(1) and 66(2) (b)		
6.1	56(3), 65(1) and 65(2) (c)		

6.1	56(4), 66(1) and 66(2) (c)		
6.1	57(3), 65(1) and 65(2) (d)		
6.1	57(4), 66(1) and 66(2) (d)		
6.1	59(2), 65(1) and 65(2) (c)		
6.1	59(3), 66(1) and 66(2) (c)		
6.1	59.1(b), 65(1) and 65(2)(e)		
6.1	59.1(c), 66(1) and 66(2)(e)		
6.1	59.2(1)(b), 65(1) and 65(2)(e)		
6.1	59.2(1)(c), 66(1) and 66(2)(e)		

6.1	59.3(b), 65(1) and 65(2)(e);			
6.1	59.3(c), 66(1) and 66(2)(e)			
6.1	59.4(1)(b), 65(1) and 65(2)(e)			
6.1	59.4(1)(c), 66(1) and 66(2)(e)			
6.1	59.5(b), 65(1) and 65(2)(e)			
6.1	59.5(c), 66(1) and 66(2)(e)			
6.1	60(b)(i), 64(1) and 64(2)(b)			
6.1	60(e), 65(1) and 65(2) (a)			
6.1	60(f), 66(1) and 66(2) (a)			

6.1	61(c), 65(1) and 65(2) (c)		
6.1	61(d), 66(1) and 66(2) (c)		
6	64.1(3)	Failure to have entered into a written agreement or arrangement with an agent or mandatary, to obtain from them the information that the agent or mandatary referred to in order to ascertain a person's identity and the information that the agent or mandatary verified as being that of the person and to be satisfied that the information is valid and current and that the person's identity was ascertained in the prescribed manner	Minor \$1-\$1,000

Table 3—Violation related to verifying the identity of parties that are not represented by a real estate broker or sales representative

Provision of the Act	Provision of the PCMLTFR	Description ⁴	Classification of violation
-----------------------------	---------------------------------	---------------------------------	------------------------------------

6.1	59.2(3)	Failure of a real estate broker or sales representative that represents a party to a prescribed transaction to ascertain the identity or confirm the existence of parties that are not represented by a real estate broker or sales representative	Minor \$1-\$1,000
------------	---------	--	----------------------

4.1 Harm done in the case of violations related to verifying client identity

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind them by identifying the individuals and entities responsible for the movement of the funds. The information collected during the process of verifying identity of an individual, or confirming the existence of an entity, must be recorded so that it can later be used to report to FINTRAC, in the RE's risk assessments and ongoing monitoring of business relationships. Verifying identity is necessary not only to meet client identification requirements, but also to meet record keeping requirements.

Verifying the identity of the parties to financial transactions and activities deters those who would launder the proceeds of crime or finance terrorist activities. When combined with the associated record keeping requirements, client identity verification also provides records and evidence for the ML/TF investigations and prosecutions of ML/TF offences.

Ultimately, without knowing the identity of the individuals involved in financial transactions potentially related to ML/TF offences, REs cannot conduct appropriate risk assessments, ongoing monitoring of business

relationships or put in place mitigation measures. Furthermore, FINTRAC and its law enforcement partners cannot follow the flow of funds to combat these illegal activities, prevent future illegal activities, and protect the integrity of Canada's financial system and the safety of Canadians.

4.2 Penalty determination for violations related to verifying client identity

The PCMLTFR set out the ways by which individuals must be identified, and the existence of entities confirmed, as well as the timelines for making these verifications. The requirements were developed to make sure that the verification of identity is done with methods that are accurate and timely, in support of FINTRAC and law enforcement agencies' purposes.

Given the importance of removing anonymity in financial transactions and activities conducted, when an RE has not taken measures to verify client identity, the maximum penalty of \$1,000 per instance will apply, as this constitutes a complete violation or disregard for the requirement.

When the methods used to verify identity are not in accordance with the methods set out in the PCMLTFR, the client's identity is considered not to have been verified, therefore the harm to achieving the objectives of the PCMLTFA and FINTRAC's mandate is the same as with not taking steps to verify client identity and the same penalty (\$1,000 per instance) will apply. Relevant mitigating factors of each case will be considered and may reduce the actual penalty amount. For example, if the RE did not verify the identity of the client within the prescribed period, but did so subsequently.

When an account is knowingly opened for a client without verifying client identity or confirming the existence of an entity, this is a violation of the prohibition under section 9.2 of the Act, which is a "serious" violation and

carries a maximum penalty of \$100,000. See *Violation related to opening an account when client identity cannot be established*.

4.3 Violations related to client identification information records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Table 4—Violations related to client identification information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	64.2	Failure of a person or entity that is required to ascertain a person's identity to keep prescribed information	Minor \$1-\$1,000
6	65(3)	Failure of a person or entity who ascertains information in respect of a corporation by referring to an electronic version of a record to keep a prescribed record	Minor \$1-\$1,000
6	65(4)	Failure of a person or entity who ascertains information in respect of a corporation by referring to a paper copy of a record to retain the record or a copy of it	Minor \$1-\$1,000

6	66(3)	Failure of a person or entity who ascertains information in respect of an entity by referring to an electronic version of a record to keep a prescribed record	Minor \$1-\$1,000
6	66(4)	Failure of a person or entity who ascertains information in respect of an entity by referring to a paper copy of a record to retain the record or a copy of it	Minor \$1-\$1,000

5. Violations related to third party determination

This section outlines FINTRAC's approach to the violations related to the requirement to make a third party determination, including the harm assessment and penalty calculation.

Table 5—Violations related to third party determination

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(1)	Failure to take reasonable measures to determine if an individual giving cash is acting on behalf of a third party	Minor \$1-\$1,000

6	9(1)	Failure to take reasonable measures when opening an account to determine if the account is to be used by or on behalf of a third party	Minor \$1-\$1,000
6	10(1)	Failure to take reasonable measures when client information record is created to determine whether the client is acting on behalf of a third party	Minor \$1-\$1,000
6	44(1)	Failure of a casino to take reasonable measures to determine if a person who receives a prescribed disbursement is acting on behalf of a third party	Minor \$1-\$1,000

5.1 Harm done in the case of violations related to third party determination

Criminals who would launder the proceeds of crime or finance terrorist activities often resort to third parties to hide their identity. By doing so, they mask their involvement in the financial transactions and activities, maintain their anonymity while giving instructions for the funds and while retaining the benefits of the funds. The PCMLTFR require RE to take reasonable measures to determine whether a transaction is being conducted on behalf of a third party, whether a client is acting on behalf of a third party or whether an account will be used for the benefit of a third party. Failing to make a third party determination may result in financial transactions and

activities being directed by unknown individuals and entities. When this occurs, REs cannot properly assess the risks posed by the transactions/activities, or report on all the parties involved in the transactions conducted. The information on third parties involved in transactions is required to be reported so that FINTRAC can properly conduct analysis to establish relationships, determine the individuals or entities directing transactions and the flow of funds, and law enforcement can effectively investigate and prosecute ML and TF offences.

5.2 Penalty determination for violations related to third party determination

The PCMLTFR require that reasonable measures be taken to make a third party determination. The reasonable measures taken must be in line with those described in FINTRAC's guidance and documented in the RE's compliance policies and procedures. As reasonable measures include simply asking the client if they are acting on someone else's behalf or retrieving information from existing records, an RE who does not take any measures to make a third party determination has fully interfered with the purpose of the requirement, which is to eliminate anonymity and identify the individuals/entities that are giving instructions on transactions/activities conducted. Given the importance of removing anonymity in financial transactions and activities, the maximum prescribed penalty of \$1,000 applies. This amount may be reduced in consideration of the relevant mitigating factors of each situation.

5.3 Violations related to third party information records

See the [guide on harm done assessment for record keeping](#) violations for the harm rationale and penalty calculation for the violations below.

Table 6—Violations related to third party information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(2)	Failure to keep a record of prescribed information respecting third parties	Minor \$1-\$1,000
6	9(2)	Failure to keep a record of prescribed information respecting third parties	Minor \$1-\$1,000
6	10(2)	Failure to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor \$1-\$1,000
6	44(2)	Failure of a casino to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor \$1-\$1,000

Table 7—Violations related to suspected third party information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(3)	Failure to keep a record of prescribed information respecting suspected third parties	Minor \$1-\$1,000
6	9(3)	Failure to keep a record of prescribed information in respect of suspected third parties	Minor \$1-\$1,000
6	10(3)	Failure to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor \$1-\$1,000
6	44(3)	Failure of a casino to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor \$1-\$1,000

6. Violation related to inter vivos trust information records

See the guide for harm done assessment for record keeping violations for the harm rationale and penalty calculation for the following violation.

Table 8—Violation related to inter vivos trust information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11	Failure of a trust company to keep a record of prescribed information concerning inter vivos trusts	Minor \$1-\$1,000

7. Violation related to beneficial ownership

This section outlines FINTRAC's approach to the violations related to the requirement to obtain prescribed information on the ownership of an entity, including the harm assessment and penalty calculation.

Table 9—Violation related to beneficial ownership

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation

6	11.1(1)	Failure to obtain the prescribed information on directors, partners or persons who own 25% or more of a corporation or other entity, and information establishing the ownership, control and structure of the entity	Minor \$1-\$1,000
---	---------	--	----------------------

7.1 Harm done in the case of a violation related to beneficial ownership

Removing anonymity and identifying the **natural** persons behind transactions and account activities is a key component of Canada's AML/ATF regime. Beneficial owners hiding behind entities, including corporations is a technique used in many ML/TF schemes. An important step in the detection, prevention and deterrence of ML/TF is the collection and verification of beneficial ownership information, which also support ML/TF investigations, and ultimately protect the integrity of Canada's financial system and the safety of Canadians.

If measures are not taken to obtain this information, there is a risk that transactions and account activities will be conducted without knowing the individuals controlling, benefitting from, or giving the instructions for the transactions. This could completely interfere with the objective of subparagraph 3(a)(i) of the PCMLTFA. This also prevents the RE from properly assessing the risks associated, law enforcement from effectively investigating and prosecuting ML and TF offences, and FINTRAC from using the information in support of its mandate, particularly in cases where the information helps establish reasonable grounds to suspect that a transaction is related to an ML/TF offence.

7.2 Penalty determination for a violation related to beneficial ownership

If an RE fails to obtain the prescribed information on the persons controlling an entity, the detection, prevention and deterrence purpose of this requirement, as described above, is completely impeded. Given the importance of removing anonymity in financial transactions and activities, the prescribed maximum penalty of \$1,000 applies. This amount may be reduced in consideration of mitigating factors for each situation.

8. Violation related to confirming the accuracy of information on the control of an entity

This section outlines FINTRAC's approach to the violation related to the requirement to confirm the accuracy of information on the control of an entity, including the harm assessment and penalty calculation.

Table 10—Violation related to confirming the accuracy of prescribed information on the control of an entity

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(2)	Failure to take reasonable measures to confirm the accuracy of the prescribed information	Minor \$1-\$1,000

8.1 Harm done in the case of a violation related to confirming the accuracy of information on the control of an entity

The requirement to take reasonable measures to confirm the accuracy of the prescribed information is not only to ensure the reliability of the information obtained, but also to deter clients from providing false information regarding the control, ownership or structure of entities. Removing anonymity from transactions is a key component of the detection, prevention and deterrence of ML and TF. Failing to take reasonable measures to confirm the accuracy of the prescribed information may result in unreliable information and in the true identity of the individuals behind transactions remaining unknown. In such situations, law enforcement cannot rely on the information to investigate or prosecute ML/TF offences, the RE cannot conduct proper risk assessments and ongoing monitoring of business relationships. In a worst case scenario, should the accuracy of beneficial ownership information be the only fact for establishing reasonable grounds to suspect that a transaction or attempted transaction is related to an ML/TF offence, it could result in an unreported suspicious transaction as that relevant suspicion would be missing. In the case where a suspicious transaction report (STR) was submitted containing beneficial ownership information in Part G that was not confirmed for accuracy, it could result in FINTRAC analyzing incomplete or inaccurate information and therefore the true flow of funds or individuals behind suspicious transactions could not be established.

8.2 Penalty determination for a violation related to confirming the accuracy of information on the control of an entity

Given the importance of removing anonymity in financial transactions and account activities, the maximum prescribed penalty of \$1,000 applies. This amount may be reduced in consideration of relevant mitigating factors of

each situation.

9. Violation related to records on beneficial ownership information

See the [guide on harm done assessment for record keeping violations](#) for the harm rationale and penalty calculation for the violation below.

Table 11— Violation related to records on beneficial ownership information

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(3)	Failure to keep a record of the prescribed information and the measures taken to confirm its accuracy	Minor \$1-\$1,000

10. Violation related to ascertaining the identity of an entity's most senior managing officer

This section outlines FINTRAC's approach to the violation related to the requirement to ascertain the identity of an entity's most senior managing officer, including the harm assessment and penalty calculation.

Table 12—Violation related to ascertaining the identity of an entity's most senior managing officer

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(4)(a)	Failure to take reasonable measures to ascertain the identity of an entity's most senior managing officer	Serious \$1-\$100,000

10.1 Harm done in the case of a violation related to ascertaining the identity of an entity's most senior managing officer

One of the most important things we can do to protect our financial system from being exploited for ML/TF purposes is to remove anonymity from financial transactions. It is important, not only to confirm the existence of an entity, but to also take reasonable measures to identify the individuals who are in control of it. When an RE is unable to obtain or confirm the accuracy of beneficial ownership information, individuals could be controlling an entity anonymously. This poses a higher risk for ML/TF offences, as individuals with criminal intent may remain undetected while potentially higher-risk activities are overlooked. Therefore, when the beneficial ownership information of an entity is not clear or cannot be established, an RE must verify the identity of the most senior person who can control the financial transactions of the entity, and treat the activities of the entity as high risk. Failing to take these additional measures could leave Canada's financial system vulnerable to ML and TF caused by individuals criminally utilizing the entities they control anonymously.

10.2 Penalty determination for a violation related to ascertaining the identity of an entity's most senior managing officer

Failing to take reasonable measures to verify the identity of the most senior managing officer and treat the activities of the entity as high risk will result in the prescribed maximum penalty of \$100,000. This amount may be reduced in consideration of relevant mitigating factors each situation.

11. Violations related to politically exposed persons (PEP) and heads of international organizations (HIO) determination

This section outlines FINTRAC's approach to the violations related to the requirement to make a determination of PEP, HIO, family member and close associate status, including the harm assessment and penalty calculation.

Table 13—Violations related to PEP and HIO determination

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
----------------------	--------------------------	-------------	-----------------------------

9.3(1)	54.2(1)(a) and 67.1(3)	Failure of a financial entity to take reasonable measures within the prescribed period to determine whether a person for whom it opens an account 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	Minor \$1-\$1,000
9.3(1)	54.2(1)(b) and 67.2(5)	Failure of a financial entity to take reasonable measures within the prescribed period to determine whether a person who requests that an electronic funds transfer of \$100,000 or more be initiated or on whose behalf the request is made is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons	Minor \$1-\$1,000

9.3(1)	54.2(1)(c) and 67.2(5)	Failure of a financial entity to take reasonable measures within the prescribed period to determine whether the beneficiary of an electronic funds transfer of \$100,000 or more is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons	Minor \$1-\$1,000
9.3(1)	54.2(2)	Failure of a financial entity to take reasonable measures on a periodic basis to determine whether an account holder 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	Minor \$1-\$1,000

6	54.2(3) and 67.1(3)	Failure of a financial entity that detects a fact that constitutes reasonable grounds to suspect that an account holder is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons to take reasonable measures within the prescribed period to determine whether they are such a person	Minor \$1-\$1,000
---	---------------------------	--	----------------------

9.3(1)	56.1 and 67.2(5)	Failure of a life insurance company or life insurance broker or agent to take reasonable measures within the prescribed period to determine whether a person who makes a lump-sum payment of \$100,000 or more in respect of an immediate or deferred annuity or life insurance policy on their own behalf or on behalf of a third party is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons	Minor \$1-\$1,000
--------	------------------	--	----------------------

9.3(1)	57.1(1) and 67.1(3)	Failure of a securities dealer to take reasonable measures within the prescribed period to determine whether a person for whom they open an account 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	Minor \$1-\$1,000
9.3(1)	57.1(2)	Failure of a securities dealer to take reasonable measures on a periodic basis to determine whether an account holder 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	Minor \$1-\$1,000

9.3(1)	57.1(3) and 67.1(3)	Failure of a securities dealer that detects a fact that constitutes reasonable grounds to suspect that an account holder is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons to take reasonable measures within the prescribed period to determine whether they are such a person	Minor \$1-\$1,000
9.3(1)	59(5)(a) and 67.2(5)	Failure of a money services business to take reasonable measures within the prescribed period to determine whether a person who requests that an electronic funds transfer of \$100,000 or more be initiated or on whose behalf the request is made is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons	Minor \$1-\$1,000

9.3(1)	59(5)(b) and 67.2(5)	Failure of a money services business to take reasonable measures within the prescribed period to determine whether the beneficiary of an electronic funds transfer of \$100,000 or more is a politically exposed foreign person, a politically exposed domestic person, a head of an international organization or a family member of, or person who is closely associated with, one of those persons	Minor \$1-\$1,000
--------	----------------------------	---	----------------------

11.1 Harm done in the case of violations related to PEP and HIO determination

A PEP or HIO is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO puts them in a position to impact policy decisions, institutions and rules of procedure in the allocation of resources and finances, which can make them vulnerable to corruption. It is important to understand that the possibility for corruption exists, and that PEPs and HIOs can be vulnerable to carrying out, or being used for, ML/TF offences.

The requirements concerning PEPs, HIOs and their family members and close associates have been put in place because of concerns about their higher vulnerability to corruption, and related higher risk of money laundering. Canada and the Financial Action Task Force (FATF) attach a

great deal of importance to the fight against corruption as it has the potential to bring great harm to economic development, the fight against organized crime and the respect for law and effective governance ⁵.

Therefore, under prescribed circumstances, financial entities; securities dealers; life insurance companies, brokers, and agents; and money services businesses are required to take reasonable measures to identify PEPs, HIOs, family members and persons closely related to them so that prescribed measures can be taken to mitigate risks. If REs fail to make the determination, risk mitigation measures cannot be applied.

11.2 Penalty determination for violations related to PEP and HIO determination

The determination of PEPs, HIOs and their family members and close associates, is the pre-requisite to taking the prescribed measures to mitigate risks. Without first making the determination, no mitigating measures can be applied and potentially higher-risk clients and their activities could remain undetected. As such, this type of violation carries the maximum penalty of \$1,000. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

12. Violations related to source of funds determination

This section outlines FINTRAC's approach to the violations related to the requirement to establish the source of funds, including the harm assessment and penalty calculation.

Table 14—Violations related to source of funds determination

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.3(2)	67.1(1)(a), (2) and (3)	Failure of a financial entity or securities dealer to take reasonable measures within the prescribed period to establish the source of funds that have been, will be or are expected to be deposited in an account	Minor \$1-\$1,000
9.3(2)	67.2(1)(a), (2) and (5)	Failure of a financial entity, life insurance company, life insurance broker or agent or money services business to take reasonable measures within the prescribed period to establish the source of funds used for a prescribed transaction	Minor \$1-\$1,000

12.1 Harm done in the case of violations related to source of funds determination

Once it has been determined that an individual is a PEP, a HIO, a family member or close associate, REs are required to determine the source of the funds that have been, will be or are expected to be deposited into an account; or to establish the source of the funds used in a prescribed transaction. The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. These requirements mitigate the inherent risks by allowing REs to know their clients, which deters criminal elements, by allowing REs to assess the ML/TF risk through the identification of the source of the funds, and through the detection of transactions that must be reported. Not complying may result in the improper assessment of ML/TF risks, which potentially leads to not applying the required mitigation measures and not reporting to FINTRAC.

12.2 Penalty determination for violations related to source of funds determination

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher risk situation has been identified. Not taking reasonable measures to determine the source of funds for these higher-risk clients will result in the prescribed maximum penalty of \$1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is

sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering no transactions have been conducted.

13. Violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

This section outlines FINTRAC's approach to the violations related to the requirement to obtain senior management approval to keep an account open, or to ensure that senior management reviews a prescribed transaction, including the harm assessment and penalty calculation.

Table 15—Violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.3(2)	67.1(1)(b), (2) and (3)	Failure of a financial entity or securities dealer to obtain within the prescribed period the approval of senior management to keep an account open	Minor \$1-\$1,000

9.3(2)	67.2(1)(b), (2), (3), (4) and (5)	Failure of a financial entity, life insurance company, life insurance broker or agent or money services business to ensure that a member of senior management reviews a prescribed transaction within the prescribed period	Minor \$1-\$1,000
--------	-----------------------------------	---	----------------------

13.1 Harm done in the case of violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. Canada and the FATF attach a great deal of importance to the fight against corruption because corruption can harm economic development; interfere with the fight against organized crime, and with respect for the law and effective governance⁶. When the approval to keep an account open is not obtained, or when a transaction is not reviewed by senior management, higher ML/TF risks may not be properly assessed and understood sufficiently to conduct effective risk assessments and to ensure that the proper mitigation measures are applied.

13.2 Penalty determination for violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher-risk situation has been identified. Failing to obtain senior management's approval to keep the account open or failing to

ensure that senior management reviews prescribed transactions in these higher-risk situations will result in the maximum penalty of \$1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

14. Violations related to records for PEPs and HIOs

See the [guide on harm done assessment for record keeping violations](#) for the harm rationale and penalty calculation for the violations below.

Table 16—Violations related to records for PEPs and HIOs

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	14	Failure to keep prescribed records	Minor \$1-\$1,000
6	14.1	<i>(Note: for Sections 14 and 14.1, specific to 14(n), 14(o) and 14.1(g))</i>	
6	23		

6	20.1	Failure of a life insurance company or life insurance broker or agent to keep a record of prescribed information when a transaction is reviewed	Minor \$1-\$1,000
6	31	Failure of a specified money services business to keep a record of prescribed information when a transaction is reviewed	Minor \$1-\$1,000

14.1 Violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

This section outlines FINTRAC's approach to the violation related to enhanced ongoing monitoring of the activity on PEP and HIO's accounts, including the harm assessment and penalty calculation.

Table 17—Violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.3(2)	67.1(1)(c) and (2)	Failure of a financial entity or securities dealer to conduct enhanced ongoing monitoring of the activities in respect of an account	Minor \$1-\$1,000

14.2 Harm done in the case of a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

When there is the potential for an increased risk of ML/TF offence, such as when a client is a politically exposed foreign person, or their family member or close associate, enhanced ongoing monitoring the client's account is a key measure that supports the detection, prevention and deterrence of ML/TF. Without enhanced ongoing monitoring, the level of scrutiny may not be appropriate to detect the transactions that would raise concern, which could result in the failure to detect the suspicious transactions or attempted suspicious transactions that are required to be reported to FINTRAC.

Ongoing monitoring must be conducted for the purposes of 1) detecting suspicious transactions that are required to be reported, 2) keeping client information up to date, 3) reassessing the level of risk, and 4) determining whether the transactions and activities are consistent with the information and risk level associated to a given client. Enhanced ongoing monitoring means that the above listed measures are conducted more frequently. When only some of the prescribed enhanced ongoing monitoring measures are conducted, or when all measures are conducted but not more frequently than for a lower risk situation, the ML/TF risks are only partially mitigated. Therefore, the penalty amount may be reduced based on the circumstances. When not performing enhanced ongoing monitoring results in the failure to report an STR, a separate violation and penalty can be imposed.

14.3 Penalty determination for a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

The penalty is set at the prescribed maximum amount of \$1,000 for each account where enhanced ongoing monitoring is not conducted. This violation poses a high level of harm to the achievement of the objectives of the PCMLTFA and of FINTRAC's mandate, since the activity on an account held by an individual identified as being vulnerable to ML/TF offences could remain overlooked; in some cases, this may also result in the failure to report suspicious transactions. This amount may be reduced in consideration of mitigating factors for each situation. For example, if no activity was conducted within the PEP or HIO's accounts prior to FINTRAC identifying the violation.

15. Violation related to ongoing monitoring of business relationships

This section outlines FINTRAC's approach to the violation related to the requirement to conduct ongoing monitoring of business relationships and to keep a record, including the harm assessment and penalty calculation.

Table 18—Violation related to ongoing monitoring of business relationships

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
----------------------	--------------------------	-------------	-----------------------------

6	54.3, 56.3, 57.2, 59.01, 59.11, 59.21, 59.31, 59.51, 60.1 and 61.1	Failure to conduct ongoing monitoring of a business relationship and to keep a record of the measures taken and information obtained	Minor \$1-\$1,000
---	--	--	----------------------

15.1 Harm done in the case of a violation related to ongoing monitoring of business relationships

The requirement to conduct ongoing monitoring of a business relationship is in place to protect REs and Canada's financial system from ML/TF.

Failing to comply with the ongoing monitoring requirement can impact the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF. When an RE fails to conduct ongoing monitoring of business relationships, it is unaware of changes to the client's transactions, activities, and circumstances; especially those that may pose a higher risk of ML/TF. When the RE is unaware, the client's information and risk assessment are not updated to reflect the true level of risk. This can potentially result in ineffective risk mitigation, and unreported transactions. When a high-risk client or business relationship is undetected because of a lack of ongoing monitoring, the RE's operations and Canada's financial system could be at risk. Should a lack of ongoing monitoring result in the failure to submit STRs, there is also an impact on FINTRAC's mandate which is to analyze and disclose information to assist in the detection, prevention and deterrence of ML/TF.

In addition, the requirement to record the measures taken and the information obtained demonstrates compliance with continuously assessing ML/TF risks, applying appropriate mitigation measures and detecting information that is required to be reported to FINTRAC. These

reports support FINTRAC's analysis and disclosure mandate, which provides valuable financial intelligence to law enforcement agencies. Not keeping a record of the information obtained would not only interfere with the purposes listed above, but could also affect law enforcement investigations and prosecutions of ML/TF if client information is not up to date.

15.2 Penalty determination for a violation related to ongoing monitoring of business relationships

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) allow for a penalty ranging from \$1 to \$1,000 for violations of ongoing monitoring requirements.

FINTRAC has identified four levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on harm done, the above-mentioned penalty range is divided in four to correspond with the identified levels of harm: \$1,000, \$750, \$500 and \$250.

The highest harm category (Level 1) is assigned the maximum amount of \$1,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the four harm levels (Level 4) has a penalty of \$250. Penalty amounts may be reduced if there are mitigating factors, but must be enough to encourage a change in compliance behaviour.

We consider all factors that may reduce a penalty to the \$1 minimum set out in the AMP Regulations.

The table below details the levels of harm, the types of non-compliance, the descriptions of harm, along with their corresponding penalties.

Table 19—Levels of harm and penalties for a violation related to ongoing monitoring of business relationships

Level of harm	Type of non-compliance	Description of harm	Penalty(not considering mitigating factors)
Level 1	No ongoing monitoring measures conducted—no detection of suspicious transactions, no update of client information, no determination whether transactions/activities are consistent, and no reassessment of risk level.	Prevents the detection, prevention and deterrence objectives of the PCMLTFA.	\$1,000
Level 2	Some ongoing monitoring measures conducted—non-compliance relates to reassessment of risk levels and determination of whether transactions/activities are consistent with information obtained.	Prevents the detection of high-risk clients, transactions and activities, making existing mitigation measures ineffective. Suspicious transactions may not be detected which could impede the detection, prevention and deterrence objectives of the PCMLTFA.	\$750

Level 3	Some ongoing monitoring measures conducted—non-compliance relates to client information update	Prevents the regime from obtaining accurate, complete, and up-to-date information on an individual/entity to assist in determining whether transactions or activities are inconsistent with what is expected for client.	\$500
Level 4	Most ongoing monitoring measures conducted on business relationships—non-compliance relates to minor record keeping	Diminishes the ability to use the information for risk assessment, risk mitigation, intelligence, compliance or investigative purposes, in a timely manner.	\$250

15.2.1 Level 1 harm—No ongoing monitoring measures conducted

In situations where no ongoing monitoring measures are taken, the potential impact on the objectives of the PCMLTFA and on FINTRAC's mandate is the greatest; therefore the harm posed is highest. As such, the penalty is determined at the prescribed maximum of \$1,000.

15.2.2 Level 2 harm—Reassessment of risk levels and transaction monitoring not conducted

In cases where some ongoing monitoring measures are taken and the non-compliance relates to the risk assessment or transaction monitoring, the harm is somewhat reduced compared to Level 1. However, this type of non-compliance could lead to the ineffective mitigation of ML/TF risks posed by the business relationship, or to the ineffective detection of suspicious transactions that need to be reported. This would pose high harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate, therefore the penalty is set at \$750.

15.2.3 Level 3 harm—Client information not kept up to date

In cases where some ongoing monitoring measures are conducted and the non-compliance relates to keeping client information up to date, the harm on the objectives of the PCMLTFA and on FINTRAC's mandate is significant, but less important when non-compliance can affect ML/TF risk mitigation. While incomplete or outdated client information can be used in transaction reports or in law enforcement investigations, higher risk transactions may still be detected, mitigated, and reported to FINTRAC for analysis. As such, the penalty is set at \$500.

15.2.4 Level 4 harm—Minor record keeping non-compliance

When ongoing monitoring measures are taken and the non-compliance relates to record keeping requirements that do not prevent the use of the information for risk assessments, risk mitigation, transaction reporting, intelligence analysis, compliance and investigations in a timely manner, the harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate is reduced. As such, the penalty is set at \$250.

16. Violations related to treating the activities of a person or an entity as high-risk

This section outlines FINTRAC's approach to the violations related to the requirement to treat client activities as high-risk and to take the prescribed special measures for mitigation, including the harm assessment and penalty calculation.

Table 20—Violations related to treating the activities of a person or an entity as high-risk

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(4)(b)	Failure to treat activities in respect of the entity as high risk and to take the prescribed special measures	Serious \$1-\$100,000
6	54.4, 56.4, 57.3, 59.02, 59.12, 59.22, 59.32, 59.52, 60.2 and 61.2	Failure to treat activities in respect of a person or entity as high risk and to take the prescribed special measures	Serious \$1-\$100,000

16.1 Harm done in the case of violations related to treating the activities of a person or an entity as high-risk

The PCMLTFR set out specific circumstances under which an RE must treat the activities of clients as high-risk and apply the prescribed special measures to mitigate the heightened risks. The prescribed special measures that are required to be taken are the development and application of written policies and procedures for taking enhanced measures, based on the risk assessment undertaken, to ascertain the identify of clients, and taking any other enhanced measures to mitigate risks including keeping client information up to date and conducting ongoing monitoring of business relationships for the purpose of detecting suspicious transactions that are required to be reported to FINTRAC. Failure to do so would mean that the necessary controls, policies and processes are not in place to for high risk situations and consequently, high-risk transactions and activities could be allowed to proceed without mitigation and reporting. This could result in STRs not being submitted to FINTRAC, and information not being available for analysis and disclosure to police and law enforcement. Ultimately, this could leave Canada's financial system and Canadians vulnerable to abuse for ML/TF purposes.

16.2 Penalty determination for violations related to treating the activities of a person or an entity as high-risk

The AMP Regulations allow for a penalty ranging from \$1 to \$100,000 for failing to treat prescribed client activities as high-risk and taking the prescribed special measures. FINTRAC has identified five levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on

harm done, the above-mentioned penalty range is divided in five to correspond with the identified levels of harm: \$100,000, \$75,000, \$50,000, \$25,000 and \$10,000.

The highest harm category (Level 1) is assigned the prescribed maximum amount of \$100,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the five harm levels (Level 5) has a penalty of \$10,000. The rationale for setting this amount as the lowest is based on the notion set out in subsection 4(2) of the AMP Regulations which establishes that a series of "minor" violations amounting to a total penalty of \$10,000 or more is considered a "serious" violation.

Penalty amounts may be reduced if there are mitigating factors, but the amount must be enough to encourage a change in compliance behaviour with respect to high-risk activities. We consider all factors that may reduce a penalty to the \$1 minimum set out in the AMP Regulations.

The table below details the levels of harm, the types of non-compliance and the descriptions of harm along with their corresponding penalties.

Table 21—Levels for harm and penalties for violations related to treating the activities of a person or an entity as high-risk

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)

Level 1	Prescribed activities not treated as high-risk and there are no policies and procedures developed for taking enhanced measures.	Prevents the ML/TF detection, prevention and deterrence objectives of the PCMLTFA. Absence of policies and procedures for high risk situations impedes the detection and mitigation of high-risk activities.	\$100,000
Level 2	Policies and procedures for taking enhanced measures are developed. However, the measures are not applied; therefore the prescribed activities are not treated as high-risk.	Prevents the ML/TF detection, prevention, deterrence and mitigation of high-risk activities. High risk situations are not being treated as high-risk because developed policies and procedures are not being applied.	\$75,000

Level 3	• Some policies and procedures for special measures are developed; • Some measures are applied; • Non-compliance relates to the failure to conduct enhanced ongoing monitoring for purposes of detecting suspicious transactions to be reported.	Prevents the comprehensive ML/TF detection, prevention, deterrence and mitigation of all high-risk activities. Affects the detection of suspicious transactions to be reported in high risk situations.	\$50,000
---------	--	---	----------

Level 4	• Some policies and procedures for special measures are developed; • Some measures are applied; and • Non-compliance relates to the failure to take enhanced measures to verify client identification or keep client information, including beneficial ownership information, up to date.	Prevents access to accurate, complete, and up-to-date client information, including beneficial ownership information. Affects the identification of persons behind the financial transactions and activities being conducted in high risk situations.	\$25,000
Level 5	• Some policies and procedures for special measures are developed; • Some measures are applied; and • Non-compliance relates to the failure to conduct any other enhanced measures to mitigate the risks identified.	Diminishes the ability to mitigate ML/TF risks, analyze or use the information for risk assessment, intelligence, compliance or investigative purposes in a timely, effective and efficient manner.	\$10,000

16.2.1 Level 1 harm—Specified client activities are not treated as high-risk and there are no policies and procedures on prescribed special measures

When an RE fails to treat prescribed activities as high-risk and there are no policies and procedures for taking enhanced measures to mitigate the risks, there is a weakness at the compliance program level which poses the most harm. If there is no system in place to ensure that enhanced measures are applied to mitigate the high risk posed by certain activities, it is more likely that the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF would be hindered. This could leave both the RE's operations and Canada's financial system more vulnerable to ML/TF. An RE in this situation would not have set out the concrete steps to take in order to reduce or prevent those risks. High-risk clients, transactions and activities could go undetected while suspicious transactions are not reported to FINTRAC. Unreported suspicious transactions lead to a loss of intelligence for investigations of ML/TF offences. Therefore the maximum penalty of \$100,000 applies under these circumstances.

16.2.2 Level 2 harm—Policies and procedures for taking enhanced measures are developed but not applied

The second highest level of harm relates to cases where policies and procedures related to taking enhanced measures for high-risk exist, but they are not being applied in practice. As mitigating measures are not taken, the prescribed activities are in fact not being treated as high-risk according to the requirements set out in the PCMLTFR. Therefore, the impact is nearly the same as in Level 1. However, an RE in this situation could more readily apply the procedures that it has developed in order to mitigate high-risk activities; therefore the harm done is potentially reduced. The penalty is \$75,000 which remains at the higher end of the prescribed range but is less than that of Level 1 harm.

16.2.3 Level 3 harm—Enhanced ongoing monitoring, for purposes of detecting suspicious transactions, not conducted

In cases where some enhanced measures are taken but the non-compliance relates to the requirement to conduct enhanced ongoing monitoring for the purpose of detecting suspicious transactions to be reported, the harm done is less than in the two previous circumstances. While other prescribed special measures are taken that could mitigate some risks, the potential unreported suspicious transactions can have a significant impact on FINTRAC's intelligence mandate, the investigation or prosecution of ML/TF offences, and other objectives of the PCMLTFA. Therefore, the penalty is set at mid-range, which is \$50,000.

16.2.4 Level 4 harm—Enhanced measures are not taken to verify client identification or keep client information, including beneficial ownership information, up to date

REs are required to take enhanced measures to ascertain the identity of clients whose activities are deemed high risk. Taking enhanced measures means doing more than what is set out in regular identity verification procedures, to ensure that the identity of the client is verified and that transactions and activities are not conducted anonymously. If an RE fails to apply these enhanced measures, some risks would not be mitigated and it could leave the RE's operations and Canada's financial system vulnerable to ML/TF. Similarly, if an RE does not take enhanced measures to keep client information up to date in situations of high-risk, outdated or incomplete information could be used in risk assessments, transaction reports, or investigations. The harm posed is less than in Level 3, as some client information is still available although not necessarily complete or up to date. As such, the penalty is set at \$25,000.

16.2.5 Level 5 harm—Other enhanced measures not taken to mitigate risks identified

When the non-compliance relates to the failure to develop and apply policies and procedures to take any other enhanced measures to mitigate the risks identified (i.e., other than performing enhanced measures to verify client identification, conduct ongoing monitoring and keep client information up to date), effective risk assessment and mitigation, and the timely and efficient availability of information for transaction reporting, analysis, compliance and investigations ML/TF are diminished. The penalty is set at \$10,000.

17. Repeated instances of a given violation

When a particular violation occurs multiple times, FINTRAC will consider its underlying cause, its type and other relevant facts to assess whether the level of harm should be reduced for the subsequent instances of that violation. For example, should repeated instances of a given violation only affect the efficiency of FINTRAC's analysis, it may be appropriate to assess its recurring instances at the base penalty of \$250 (level 4 harm), regardless of the level of harm of the first occurrence.

Footnotes

- 1 See section 3 of the Act.
- 2 See section 40 of the Act.
- 3 The description is for reference only. Refer to the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) for the official Short-form description of the violations.

- 4 The description is for reference only. Refer to the AMP Regulations for the official Short-form description of the violations.
 - 5 FATF: Corruption, <https://www.fatf-gafi.org/en/topics/corruption.html>
 - 6 FATF: Corruption, <https://www.fatf-gafi.org/en/topics/corruption.html>
-

Date Modified:

2019-08-26