



**CRAWFORD
SMITH &
SWALLOW**

Chartered Professional
Accountants LLP

**FINTRAC
CANAFE**



**Financial Transactions and
Reports Analysis Centre of Canada**

**Centre d'analyse des opérations
et déclarations financières du Canada**

CSS AML/ATF Compliance Policy Manual

Table of Contents

<u>1.</u>	<u>BACKGROUND AND LEGAL FRAMEWORK</u>	<u>4</u>
	<i>Proceeds of Crime (Money Laundering) & Terrorist Financing Act (PCMLTFA) & Associated Regulations</i>	<i>4</i>
<u>2.</u>	<u>GENERAL POLICIES AND SUPPORTING PROCEDURES</u>	<u>5</u>
	<i>Welcome</i>	<i>5</i>
	<i>Terminology Used in This Manual.....</i>	<i>5</i>
	<i>Background</i>	<i>5</i>
	<i>Accountability and Commitment</i>	<i>6</i>
	<i>Client Awareness.....</i>	<i>7</i>
	<i>AML/ATF Compliance Program.....</i>	<i>7</i>
	<i>Risk-Based Approach.....</i>	<i>10</i>
	<i>Compliance Officer (CAMLO/Deputy CAMLO) Appointment</i>	<i>11</i>
	<i>Compliance Training Program and Plan</i>	<i>13</i>
	<i>Independent Biennial Review of AML Compliance Program.....</i>	<i>14</i>
	<i>FINTRAC Compliance Examinations:</i>	<i>16</i>
<u>3.</u>	<u>COLLECTING CLIENT IDENTIFICATION INFORMATION & RECORDS</u>	<u>17</u>
	<i>Background</i>	<i>17</i>
	<i>Client Identification.....</i>	<i>17</i>
	<i>PEPs and HIOs</i>	<i>22</i>
	<i>Business Relationships</i>	<i>26</i>
<u>4.</u>	<u>REQUIRED REPORTING POLICY</u>	<u>27</u>
	<i>Background</i>	<i>27</i>
	<i>Suspicious Transaction Reporting (Completed and Attempted)</i>	<i>28</i>
	<i>Required Reporting Policy.....</i>	<i>31</i>
	<i>Immunity from Prosecution (STRs).....</i>	<i>32</i>
	<i>Unauthorized Disclosure of Suspicious Transaction Reports (Completed or Attempted)</i>	<i>32</i>
	<i>Publicly Available Information and STR Submissions.....</i>	<i>32</i>
	<i>Credible Sources Information and STR Submissions.....</i>	<i>32</i>
	<i>Listed Person and Entity Property Reports (LPEPR).....</i>	<i>33</i>



	<i>Immunity from Prosecution (LPEPR)</i>	<i>33</i>
	<i>Economic and Trade Sanction Monitoring Restrictions</i>	<i>35</i>
5.	<u>REQUIRED RECORD KEEPING POLICY.....</u>	<u>36</u>
	<i>Background</i>	<i>36</i>
6.	<u>PENALTIES FOR NON-COMPLIANCE POLICY</u>	<u>38</u>
	<i>Penalties for Non-compliance</i>	<i>38</i>
7.	<u>APPENDICES</u>	<u>40</u>
	<i>APPENDIX A: POSSIBLE ML/TF INDICATORS FOR THE ACCOUNTING SECTOR</i>	<i>40</i>
	<i>APPENDIX B: SUGGESTED READING.....</i>	<i>44</i>
	<i>APPENDIX C: GLOSSARY OF TERMS & ABBREVIATIONS.....</i>	<i>45</i>

1. BACKGROUND AND LEGAL FRAMEWORK

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

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* received royal assent on June 29, 2000. The Act established a mandatory transaction-reporting program where suspicious transactions and or prescribed reports are sent to an independent government agency – **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**. The Centre's mandate is to collect, analyze, and produce case disclosure information to assist in the detection, prevention and deterrence of money laundering and terrorist financing in Canada and abroad.

The PCMLTFA is supported by the following Regulations:

- The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations. <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>
- The Cross-Border Currency and Monetary Instruments Reporting Regulations. <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations. <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations. <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>
- FINTRAC Assessment of Expenses Regulations: <https://fintrac-canafe.canada.ca/act-loi/1-eng#s2>

Since its original in-force date additional changes, enhancements and new requirements have been added to the legislation on a continuous and consistent basis.

Other Canadian organizations involved in combatting Money Laundering and Terrorist Financing:

- Royal Canadian Mounted Police (RCMP): <http://www.rcmp-grc.gc.ca>
- Canada Border Services Agency (CBSA): <http://www.cbsa-asfc.gc.ca>
- Canada Revenue Agency (CRA): <http://www.cra-arc.gc.ca>
- Canadian Security and Intelligence Service (CSIS): <http://www.csis-scrs.gc.ca>
- *Global Affairs Canada*: <https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=eng>
- Public Safety Canada (PSC): www.publicsafety.gc.ca
- Department of Finance Canada: <https://www.canada.ca/en/departement-finance.html>

2. GENERAL POLICIES AND SUPPORTING PROCEDURES

Welcome

If you have just recently joined us or even have been with us for a while, on behalf of Crawford Smith & Swallow Chartered Professional Accountants LLP (“**FIRM**” or “**CSS**”) and your fellow team members, please accept our warmest welcome. Members of the CSS team (“**Team Members**” or “**Staff**”) work together, sharing responsibilities and pooling their skills, knowledge, and efforts to achieve common goals.

We trust that you will take pride in being a member of our team and that your experience with us will be challenging, enjoyable, and rewarding.



Crawford Smith & Swallow Chartered Professional Accountants LLP

Terminology Used in This Manual

When you sign off on CSS AML/ATF Compliance Policy Manual, you are signing an agreement acknowledging that you have read and understand the policies included in this manual and that you agree to adhere to them. So, it is important you understand the terminology used in this manual as it uses certain terms that have specific formal meanings. Rather than defining a formal term each time it is used in this Manual, they are defined in a separate section at the end of this document called [Glossary of Terms](#).

Background

CSS and its employees and partners have reporting responsibilities to FINTRAC when engaged in any of the following activities on behalf of an individual or entity, **or** give instructions on behalf of a person or entity in respect of:

- Receiving or paying funds or virtual currency;
- Purchasing or selling securities, real property or immovable or business assets or entities;
- Transferring funds, virtual currency or securities by any means;

When CSS **gives instructions** for any of the triggering 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."

Audit, review and compilation engagements carried out in accordance with the CPA Handbook do not trigger any reporting responsibilities. Providing bankruptcy services or acting as an insolvency practitioner does not trigger reporting obligations.

INTERNAL CSS RISK CONTROLS VS. FINTRAC LEGAL TRIGGERS

Audit, review, compilation, tax, advisory, and similar professional services may be risk-rated internally by CSS for AML/ATF control purposes. However, these services do not by themselves trigger FINTRAC accountant obligations unless CSS engages in, or gives instructions for, a prescribed activity, including receiving or paying funds or virtual currency, purchasing or selling securities, real property, business assets or entities, or transferring funds, virtual currency or securities.

The Compliance Program stipulated under Section 71(1)(b) of the ***Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*** sets out that all organizations must put in place "... **effective policies and procedures to prevent, detect and address non-compliance**". As an Accounting Practice engaged in the provision of designated services governed under Canada's Money Laundering legislation, our approach is to ensure compliance with the PCMLTFA, its associated Regulations and FINTRAC's AML/ATF compliance program Guidance.

Accountability and Commitment

POLICY

The partners, management and staff members of Crawford Smith & Swallow LLP (CSS) are committed to meeting and maintaining all relevant accounting Firm compliance requirements set under The Act and its various supporting Regulations.

PROCEDURES

AREA	ACTIVITY	RESPONSIBILITY
Management	• The Equity Partners (EP) have put in place all necessary elements of a FINTRAC compliance program.	Equity Partners
	• The Chief Anti-Money Laundering Officer (CAMLO) will inform all employees of the company plans for compliance.	CAMLO
	• The CAMLO will subscribe to FINTRAC's news releases to keep up to date on new legislative developments, policies, guidance, ministerial directives, transaction restrictions/prohibitions, typologies and procedures.	CAMLO

Client Awareness

POLICY

Crawford Smith & Swallow makes every effort to inform clients of its responsibility to comply with Canada's AML/ATF program by reporting prescribed transactions, verifying proof of identification from prospective clients, and keeping important records/documents relevant to all designated transactions governed by the PCMLTFA and associated Regulations.

PROCEDURES

AREA	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none"> Ensure that client questions with respect to practice compliance under the PCMLTFA are answered and that their personal information is safeguarded. 	CSS Partners, Management and Employees

AML/ATF Compliance Program

POLICY

FINTRAC's Compliance Program Requirements stipulates that designated accounting firms are required to implement all six elements of the AML/ATF Compliance Program. This policy confirms that Crawford Smith & Swallow intends to adhere to this requirement and implement the legislated elements.

PROCEDURES

AREA	ACTIVITY	RESPONSIBILITY
Management	<ol style="list-style-type: none"> A Chief Anti-Money Laundering Officer (CAMLO) has been appointed, supported by a Deputy CAMLO. Compliance Policies and Procedures are in place and has senior management approval and endorsement of their operationalization. A money laundering and terrorist financing risk assessment has been developed that measures the Firm's regulated services and identifies the impact of possible ML/TF risks and applies controls and measures to mitigate these risks. 	Managing Partner Compliance Team Compliance Team



	4. Develop and maintain a written, ongoing compliance training program for your employees, agents or mandataries, or other authorized persons.	Compliance Team
	5. Institute and document a plan for the ongoing compliance training program and deliver the training (training plan)	Compliance Team
	6. The Firm undertakes an independent effectiveness Review of its compliance program biennially.	Compliance Team

The CSS AML/ATF Compliance Program is supported by the AML/ATF Compliance Policy Manual, AML/ATF Risk Assessment Manual, Client On-Boarding Risk Questionnaire, Monitoring Record, Individual Verification Form, Entity & Beneficial Ownership Verification Form, Risk Assessment Screening Guide, training records, effectiveness review documentation, and related compliance procedures.

Obligation	Trigger	Responsible Person	Form/Record	Deadline
Client ID	Prescribed activity / business relationship	Engagement team	Individual or Entity Verification Form	Before proceeding where required
Beneficial ownership	Entity client	Engagement team	Entity & BO Form	Before or during onboarding
PEP/HIO/sanctions	New client / reassessment / trigger event	Engagement team + CAMLO	Screening record	Before proceeding / upon trigger
STR	Reasonable grounds to suspect ML/TF	CAMLO	STR file	As soon as practicable
LCTR	CAD \$10,000+ cash or 24-hour rule	CAMLO	ROF + LCTR record	Within 15 calendar days after receipt of cash, where LCTR applies
Monitoring	Ongoing relationship	Engagement team	Monitoring Record	Based on risk rating
Effectiveness review	Every 2 years	Independent reviewer	Review report	Biennially
Training	New staff and ongoing	CAMLO/Deputy CAMLO	Training record	At onboarding and annually/periodically

Risk-Based Approach

POLICY

The PCMLTF Regulations, as covered under Section 3 of FINTRAC's Compliance Program Requirements, specify that an accounting Firm should include a documented assessment of risks related to money laundering and terrorist financing. To that end, in an effort to institute enhanced due-diligence, CSS is committed to implement an approach to manage risk with respect to identifying potential vulnerabilities of money laundering and terrorist financing by assessing its services, delivery channels, location and clients.

This process encompasses the following:

- the risk assessment of services, clients, delivery channels and geographic locations of the Firm and its clients; as well as other associated risks that impact on CSS's business activities and business relationships;
- assessing the risks resulting from new developments or new technologies that CSS intends to carry out or introduce, before doing so, that may have an impact on our practice;
- put in place the risk-mitigation to implement controls to handle identified risks from both entity and individual clients;
- keeping client identification up to date; and
- the ongoing monitoring of higher-risk clients, business relationships, engagements, and trigger events, as the risk assessment is a dynamic process.

For all clients assessed as **high risk**, CSS will review their account, at a minimum, every **12 months**. For clients assessed as **medium risk**, CSS will review their account every **two years**. And **low risk** clients are reviewed every **three years**. For all risk-level clients, risk mitigation procedures are identified, documented and discussed in greater detail in the *CSS Risk Assessment Manual*.

In addition, the CSS compliance management team makes it a practice to randomly test samples of clients from all risk levels to confirm their respective risk rating continues to remain at the assigned level or needs to be changed to reflect the risk impacts found during the testing process. This test sampling process is set out in the Risk Assessment Manual.

PROCEDURES

AREA	ACTIVITY	RESPONSIBILITY
Management	<ul style="list-style-type: none"> • Development of a risk-assessment methodology tool (risk matrix) to score all of our practice services, clients, geographic locations and delivery channels. 	Compliance Team Compliance Team



	<ul style="list-style-type: none"> Conduct client risk assessments with all clients where a business relationship has been determined and assign each of those clients a risk score to be managed using risk mitigation activities assigned to each risk level. 	
	<ul style="list-style-type: none"> Compliance will update and maintain the Risk Assessment Program annually. Any changes are subsequently approved by the Equity Partners committee. 	Compliance
	<ul style="list-style-type: none"> Clients who qualify for the 'Business Relationship' arrangement with CSS will be risk rated using the <i>Appendix A – Client On-Boarding Risk Questionnaire in the CSS AML/ATF Risk Assessment Manual</i> Based on the score from that questionnaire, the client will be assigned a risk rating of high, medium or low. 	Compliance
	<ul style="list-style-type: none"> Each client's risk rating will be recalculated at each scheduled BR review, when a trigger event occurs or if selected for the CSS sample risk testing exercise. 	Compliance
	<ul style="list-style-type: none"> CSS has identified specific client factors that automatically default to a high risk rating (e.g., PEP or HIO standing, a filed STR having taken place, etc.). 	Compliance
	<ul style="list-style-type: none"> All high risk rated clients who are Foreign PEPs/HIOs will remain high risk forever. 	Compliance

It is important to note that high-risk business relationships are subject to enhanced transaction monitoring (ETM) and mitigation measures. For example, as noted above activity for all high-risk clients and business relationships are reviewed at least annually, and more frequently when further triggered by other unusual client activity. We also Conduct client risk-assessments in situations where a client might be acting on behalf of a third party or entity and when a corporation will not identify the beneficial owners.

The compliance team will test to ensure the mitigating factors identified in the Firm-wide Reporting Risk Assessment Program are being applied and proper documentation is made on the Monitoring Record and applicable client risk assessment documentation.

NOTE: *The Risk Assessment (RA) Program is described in a separate Risk Assessment Manual, which sets out the various requirements of the RA to CSS operations.*

Compliance Officer (CAMLO/Deputy CAMLO) Appointment

The PCMLTFA Regulations, as covered under *Section 1 of FINTRAC's Compliance Program Requirements*, states that reporting entities appoint a designated Compliance Officer (CAMLO) to oversee the risk-based compliance program. This Compliance Officer should have direct access to the accounting Firm's senior practice partners.

The CAMLO is an individual in the Firm who is responsible for the implementation and review of the compliance program. The CAMLO should have knowledge of CSS's function and structure as well as the accounting sector's ML/TF risks and vulnerabilities and trends and typologies. This individual shall ensure

that all Firm staff with client contact have a full understanding of their responsibilities. The CAMLO reports to the Firm's Managing Partner. The CAMLO will be assisted by a Deputy CAMLO who will be responsible for the compliance program in the CAMLOs absence.

The Firm's Equity Partner group appointed the following individuals to the CAMLO and Deputy CAMLO positions:

CAMLO: Susanne MacMahon

Deputy CAMLO: Jennifer Bailey

The duties of the CAMLO include the following:

- Register with FINTRAC and obtain an ID number, logon ID, and password for reporting purposes when a designated report needs to be filed using the FWR system;
- File all necessary reports with FINTRAC relating to suspicious transactions (completed or attempted), single or cumulative large cash transactions, other prescribed reports, where applicable (incoming or outgoing) or listed person and entity property transactions;
- Maintain all designated records as required under the legislation and FINTRAC guidance;
- Implement, administer and maintain the CSS AML/ATF compliance program;
- Ensure that all of employees and Partners receive training and keep a record to that fact; thereby, ensuring all employees and partners receive ongoing training as required to remain current with legislative changes or changes to our Firm's policies and procedures;
- Prepare any necessary forms to facilitate reporting by employees to the CAMLO;
- Regularly monitor identified websites for lists of terrorist individuals and organizations and inform employees, partners, and other personnel with respect to changes on those lists;
- Review and update all practice compliance program manuals and documents annually to ensure they are current with the legislation, FINTRAC's Guidance and our business practices;
- Regularly monitor relevant AML/ATF websites, participate in training seminars and read compliance management resources to ensure that the CAMLO, and Firm employees and partners are kept up to date at all times; and
- Manage the required Compliance Effectiveness Review every two years according to FINTRAC's designated schedule.

The CAMLO can assign and/or share any of the above responsibilities with the Deputy CAMLO to ensure the compliance program is maintained in a current, complete and effective manner.

POLICY:

Crawford Smith & Swallow LLP has designated a Chief Compliance Officer (CAMLO) and Deputy CAMLO who are jointly responsible for all AML/ATF compliance activities across the Firm. In their roles, they can assign designated AML compliance responsibilities to other employees and partners when compliance operational efficiency and effectiveness deems it appropriate.

Compliance Training Program and Plan

The PCMLTF Regulations, as covered under *Section 4* of FINTRAC's *Compliance Program Requirements*, requires that accounting firms develop a written training program for employees and partners who engage in any business services offered by the Firm governed under the Act. To that end, an ongoing AML/ATF compliance training program is maintained by the CAMLO for all employees, partners and external consultants who have contact with clients, who see client transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance program.

POLICY:

The partners, management and staff members of CSS are committed to meeting and maintaining all relevant accountant training requirements set under The Act, its supporting Regulations and FINTRAC Guidance.

Currently, CSS subscribes to the web-based AML/ATF Training Course for the Accounting sector delivered by ABCsolutions through its COMPLY-LMS training platform. The training program covers the following topics from both a general and a sector-specific perspective:

- Defining and describing money laundering and terrorist financing;
- Key Canadian agencies involved in detecting, fighting and deterring money laundering and terrorist financing;
- Identifying elements of the Firm AML/ATF Compliance Program;
- Understanding AML/ATF risks of an accountant Firm and the elements of the Firm's Risk-Based Approach and Risk Assessment Program
- Reporting, client identification, record-keeping and business relationship responsibilities; and,
- An overview of both criminal and civil penalties that apply to compliance deficiencies and avoidance.

This training program has a testing capability drawing questions at random from a large question databank developed for each module in the course. Consequently, every time an individual signals they wish to take a module test a new set of questions is randomly selected. Each test score is recorded in the COMPLY-LMS administration back office and can be reviewed by CSS training administrators to follow staff progress. A score of 80% has been assigned as the passing grade for each course module and the final test required to successfully complete this component of the firms training activities. This training program/resource is renewed annually with the third-party service provider.

In addition, accountant-specific AML/ATF learning documents developed outside of the web-based training modules are uploaded and maintained as current in a 'Document Resource Section' on the COMPLY-LMS training and testing platform available to all users 24/7 through a password access system.

An annual CSS **training plan** will be filled in as training events occur, scheduled and impromptu, within the Firm. The training activities will be recorded using a **Training Log Worksheet** developed for that process. The Log will include the various information details set down by FINTRAC in Guideline 4, Section 6 addressing training recipients, topics, materials, delivery methods and frequency.

CSS has implemented the following procedures, with respect to its training requirements:



PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none"> Implement and sustain as current an on-going web-based, AML/ATF compliance training program and plan for Firm employees, partners and engaged consultants. 	Compliance and Training Service Provider
	<ul style="list-style-type: none"> Ensure all new hires and returning staff successfully complete the AML/ATF Training course before they undertake regulated services for clients. 	Compliance Team
	<ul style="list-style-type: none"> Monitor the web-based training course result logs and work with those staff members who are under performing in their test results (method of delivery). 	Compliance Team
	<ul style="list-style-type: none"> Undertake an annual review of the training program to ensure it remains applicable to the CSS compliance program requirements. 	Compliance Team
	<ul style="list-style-type: none"> Put in place an Annual Training Plan using the Training Log Worksheet and keep it current with every training activity undertaken. 	Compliance Team
	<ul style="list-style-type: none"> Ensure all legislation and/or practice compliance program changes, enhancements and edits are passed on to and reviewed by all employees and partners; as well as being added to the Training Log Worksheet. 	Compliance Team
	<ul style="list-style-type: none"> Ensure that resources are requested to ensure the compliance teams in-service training needs are met to maintain their subject matter status in the Firm. 	Compliance Team and Equity Partners Group
	<ul style="list-style-type: none"> To put in place a communication process across the Firm to manage, record and store all legislative, regulatory and Guidance updates impacting the CSS compliance program and its delivery. 	Compliance Team

Independent Biennial Review of AML Compliance Program

FINTRAC's *Compliance Program Requirements* stipulate in *Section 5* that a comprehensive compliance program should be reviewed and tested for its completeness, applicability, currentness and effectiveness biennially. This review should be done by an external resource experienced in the requirements of a Firm AML/ATF compliance program who is independent of the actual program operations and management.

The results of the review must be reported to the Equity Partners Group within 30 days after the completion of the review, including an action plan setting out all required updates to the various Manuals, records, reporting requirements, client KYC practices and business risks identified as having limitations and/or deficiencies in the Review Report findings. Failure to complete, document, or report required

compliance review activities may result in regulatory findings, administrative monetary penalties, or other enforcement action, depending on the nature and severity of the non-compliance.

POLICY:

CSS will arrange for a scheduled Biennial Effectiveness Review every two-years. The Review will be contracted out to an external consultant with subject matter expertise and experience in the AML/ATF compliance field and managing the Review process. This review will cover all the elements in the CSS Compliance Management Program and will be overseen by the Firm's compliance team.

PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none"> Schedule an external Compliance Review every two years. 	Compliance Team
	<ul style="list-style-type: none"> Identify an external Compliance Consultant to perform the Compliance Review. 	Compliance Team
	<ul style="list-style-type: none"> A formal, <i>Response Action Plan</i>, setting out Review Recommendations and Approved remediation activities, will be prepared and subsequently approved by the Equity Partner Group. This will be provided as part of the documentation for the next scheduled Biennial Compliance Review to enable the Reviewer to confirm whether the action plan has been completed as set out. 	Compliance Team
	<ul style="list-style-type: none"> Ensure that the Compliance Review results, recommendations, and proposed remediation actions are shared with the Equity Partner Group within 30 days of receiving the Final version of the Review Report. 	CAMLO and Equity Partner Group
	<ul style="list-style-type: none"> Upon receiving approval from the Equity Partner Group, implement all corrective actions along with the detailed timelines. 	Compliance Team
	<ul style="list-style-type: none"> All Biennial Review Reports and their associated Action Plans will be provided if requested by FINTRAC for a forthcoming Compliance Examination review, within the stipulated 30 day requirement. 	Compliance Team

On an additional program effectiveness note, the compliance team performs an internal review on an annual basis of the Policy & Procedure and Risk Assessment Manuals to ensure any and all necessary updates and additions have been made as they come into force. In addition, compliance will undertake sample testing of client records, reports, KYC practices, scheduled business relationship reviews, PEPs/HIO and designated individual and entity reporting list searches to confirm each is effectively doing what is intended.

FINTRAC Compliance Examinations:

The PCMLTFA gives FINTRAC special powers to “inquire into the business” of all reporting entities in every sector that have legislative obligations. FINTRAC’s compliance monitoring is essentially cooperative; but businesses like Crawford Smith & Swallow LLP must grant access to FINTRAC officials and provide ‘reasonable assistance’ when requested as part of a Compliance Examination.

POLICY:

Crawford Smith & Swallow LLP is committed to being compliant with the PCMLTFA and associated Regulations when it comes to cooperating with FINTRAC officials tasked with undertaking a compliance examination of its compliance program. All assistance will be coordinated through the Firm’s CAMLO.

PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none"> Enforce the practice records retention policy to ensure documents can be retrieved for the FINTRAC Examination when requested. 	CAMLO
	<ul style="list-style-type: none"> Coordinate the FINTRAC examination on behalf of the practice, including ensuring that all records and reports are available to FINTRAC officials. 	CAMLO
	<ul style="list-style-type: none"> Develop a plan of action for corrective measures emanating out of the Compliance Examination findings. Ensure that the action plan is approved by the Equity Partner Group. 	CAMLO
	<ul style="list-style-type: none"> Ensure that all examination findings and Action Plan Response Activities are kept on file indefinitely and made available when asked as a part of a future Examination or Biennial Compliance Review. 	CAMLO

3. COLLECTING CLIENT IDENTIFICATION INFORMATION & RECORDS

Background

The PCMLTFA Regulations require that accounting firms and their employees who engage in the regulated activities verify client identification, keep records, and ensure that these records are kept up to date. This includes obtaining information, supported by required and approved documentation from clients who undertake a regulated transaction with the Firm.

CSS has client identification responsibilities to FINTRAC when engaged in any of the following activities on behalf of an individual or entity or give instructions on behalf of a person or entity in respect of:

- Receiving or paying funds;
- Purchasing or selling securities, real property or immovables or business assets or entities; or
- Transferring funds or securities by any means.

Measures must be taken to verify the identity of individuals and to confirm the existence of entities when CSS is engaged in any of the above type transactions. Once we have verified the identity of the individual or entity, CSS is not required to verify their identity again unless required to do so by regulation or Guidance. However, in the case of an individual, CSS management or staff must be able to recognize the individual (visually or by voice) at the time of a future event. Any doubts would require verifying their identity again.

The identity does not need to be verified for Canadian provincial or federal departments or Crown agencies, incorporated Canadian municipal bodies, hospital authorities and for large corporations with a minimum of \$75 million on its last audited balance sheet. The large corporation must also be traded on the Canadian stock exchange or another stock exchange as designated by the Minister of Finance and operate in a country that is a member of the Financial Action Task Force.

Client identification is required for large cash transactions, virtual currency transactions, suspicious transactions and the receipt of funds record. For more information on this, see sections 3 and 4.

NOTE: *CSS does not undertake large cash transactions nor virtual currency transactions.*

NOTE: *Once CSS has completed two transactions that require verifying the identity of the client, a **business relationship** (BR) has been formed. Business relationships are discussed in greater detail later in this section and in the CSS AML/ATF Risk Assessment Manual.*

Client Identification

POLICY:

Partners, managers and staff are required to ensure that the customer identification procedures have been performed for all clients of CSS in accordance with the Act and its Regulations for those transactions identified in the Background information above.

- Where possible, partners, managers and staff will perform customer identification procedures prior to engaging in a transaction that fall into the receipt of funds definition (see Section 4).
- Partners, managers and staff will take reasonable measures to verify the identity of an individual who conducted or attempted to conduct the transaction. This is not required if you have already verified the identity of the individual and you have no doubts about that identification information or if you believe verifying their identity would inform the individual that you are submitting a suspicious transaction report.
- Where a business relationship has been developed, partners, managers and staff are to ensure that the information previously recorded on the client's file remains accurate.

CSS has both individual and entities as clients. CSS has determined that the following documents set out in the following Table are considered acceptable as a source of identification, for the client categories listed. The final column sets out the information that must be documented by partners, managers and staff when collecting client identification.

Client Type	Valid and Preferred Documents used for Client ID	Documentation Detail Requirements	Documentation Requirements to be Recorded
Individuals: Physically present	Use Government-issued photo identification method: Document must be authentic, valid and current. Photo identification issued by federal or provincial government including: <ul style="list-style-type: none"> • Driver's licence • Passport • Permanent resident card • Provincial or territorial identity card • Other similar documents with photo identification • Equivalent foreign documents are acceptable 	<ul style="list-style-type: none"> • Name and photograph must match • Cannot be expired • Must be valid - unaltered • Reference number must be available • An authentic document (not a photocopy) 	<ul style="list-style-type: none"> • Individual's name • Date of verification • Type of document • Document number • Province, state or country that issued the document • Expiry date (if applicable)
Individuals: Not physically present **	Use Government-issued photo identification method OR use Dual Process Method: Request two documents. <ul style="list-style-type: none"> • Each document must confirm one of the following but cannot confirm the same option (for example, you cannot use two separate 	<ul style="list-style-type: none"> • Name, address and date of birth must match information previously given to you by the client • Documents must be valid and current • Documents must be from two independent and reliable sources (for 	



	<p>documents that only confirm the name and date of birth):</p> <ul style="list-style-type: none"> • Name and date of birth • Name and address • Name and financial account <p>Valid documents include (for a full list, contact compliance):</p> <ul style="list-style-type: none"> • CPP statement • Property tax assessment • CRA notice of assessment • Utility bill • Credit file in existence for at least 6 months • Insurance documents (home, auto, life) • Birth certificate • Permanent resident card • Bank statement • Credit card statement • Record of employment 	<p>example, you cannot have two documents from the CRA)</p>	
<p>Corporations: Confirmation of existence method</p>	<p>Information is authentic, valid and current One of the following to confirm name and address:</p> <ul style="list-style-type: none"> • certificate of incorporation • certificate of corporate status • record that has to be filed annually under provincial securities legislation • published annual report signed by an audit Firm • letter or notice of assessment from a municipal, provincial, territorial or federal government <p>And one (1) of the following to confirm the directors:</p> <ul style="list-style-type: none"> • Electronic document from public source such as federal database(Corporations Canada database) or by subscribing to a corporation searching and registration service • List of corporation's directors submitted with application for incorporation 	<ul style="list-style-type: none"> • Document used to confirm identity and directors can be paper or electronic (not verbal) • Name and address of corporation and Names of Directors must match the document obtained 	<p>If CSS staff consulted an electronic record include the:</p> <ul style="list-style-type: none"> • registration number; • type of document consulted; and • the source of the electronic document. <p>If you consulted a paper record include:</p> <ul style="list-style-type: none"> • the paper record, or a copy of the record



	<ul style="list-style-type: none"> • Updated list of directors from client's minute book 		
Trusts, Partnerships, Funds, Unincorporated Associations/Organizations Confirmation of existence method	<ul style="list-style-type: none"> • Partnership agreement • Articles of association • Any other similar record that confirms the entity's existence • Letter or notice of assessment from a municipal, provincial, territorial or federal government 	Confirmed by paper or electronic document (not verbally) <ul style="list-style-type: none"> • Electronic documents must come from a public source • Name and address of the entity must match the documents obtained 	If you consulted an electronic record: <ul style="list-style-type: none"> • registration number; • type of record consulted; and • source of the electronic Record If you consulted a paper record: <ul style="list-style-type: none"> • the paper record, or a copy of the record

****Where an individual is not physically present, the Government-Issued Photo Identification Method may be used provided reasonable measures are taken to authenticate the document and confirm that the name and photograph match the individual. The Dual Process Method may be used where government-issued photo identification is unavailable or where circumstances warrant its use.**

Beneficial Ownership

Identifying beneficial ownership is important in order to remove anonymity and identify the actual individuals behind transactions and business activities, which is a key component of Canada's anti-money laundering and anti-terrorist financing regime. The concealment of the beneficial ownership information of accounts, businesses and transactions is a technique used in money laundering and terrorist activity financing schemes. Consequently, the collection and confirmation of this information is a crucial step to aid in money laundering and terrorist activity financing investigations and ultimately protect the integrity of Canada's financial system. It also contributes to the risk mitigation associated with our firms clients.

Each time CSS employees and partners have to confirm the existence of an entity, they will obtain and/or take reasonable measures to confirm and keep records of the information about the entity's beneficial ownership. Specifically:

1. **Corporation:** confirm the names of all directors of the corporation, and the names and addresses of all actual persons who own or control, directly or indirectly, 25 percent or more of the entity.
2. **Trust:** confirm the names and addresses of all trustees, known beneficiaries and settlors of the trust, and whether no percentage of ownership is required in this situation.
3. **An entity is a business other than a corporation or trust:** confirm the name and addresses of all individuals who own or control, directly or indirectly, 25 percent or more of the entity.
4. **Not-for-profit organization:** in addition to that required in (3), you must also identify if it is a charity registered with the Canada Revenue Agency or if it is an organization that solicits charitable donations from the public.

NOTE: Since a beneficial owner ***cannot be*** another corporation or entity, it may require reviewing several levels of documentation to determine the actual beneficial owners.



The details of the various activities that must be taken with respect to beneficial ownership can be found set out in the Web-based *AML/ATF Training Module Four: Client Identification and Record Keeping Requirements*.

POLICY:

CSS will identify the beneficial ownership of all corporate, trust and non-incorporated business clients in accordance with the Act and its Regulations.

PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none">CSS will confirm beneficial ownership when the identity of an entity is being confirmed.CSS will capture and record information establishing the ownership, control and structure of the entity as noted above.CSS will confirm the accuracy of the information collected by referring to such documents as: Minute Book, shareholders register, articles of incorporation, shareholder agreements, partnership agreements or BOD meeting records of decisions.When beneficial ownership information is not provided or cannot be confirmed as to its accuracy, CSS will use reasonable measures to verify the identity of the chief executive officer (CEO) or of the person who performs that function; and apply the special measures for high-risk clients, including enhanced ongoing monitoring. A record of the steps taken to identify the CEO will be made.CSS will keep a record in those circumstances where no individuals hold more than 25% or greater ownership of a corporation and will document the date that the measures were taken.	Partner or Employee tasked with capturing the client's information

Corporations Assigned a High Risk Rating and Beneficial Ownership

When a corporate client enters into a Business Relationship status with CSS its degree of risk must be assigned. If the risk is set at **high** then CSS must consult Corporations Canada's database when we first determine there is a high risk and in the course of conducting ongoing monitoring of our high risk clients business relationships.

When consulting Corporations Canada's database, CSS will compare the information we obtained on the corporation to the individuals with significant control of the corporation listed in Corporations Canada's database and determine if there is a material discrepancy. Now what is a material discrepancy? Specifically, FINTRAC Guidance indicates that *"A material discrepancy is a meaningful inconsistency between the beneficial ownership information of a corporation incorporated under the Canada Business*

Corporations Act and the individuals with significant control listed in Corporations Canada's database that could impact the proper identification, or conceal, the individuals that own or control a corporation."

What is a material discrepancy? It does not include a discrepancy that arises from: a spelling mistake or minor variation in a name or address; the use of a service address in one information source and a residential address in another; the fact that information is not available to the public due to an exception or exemption; the presence of an exception or exemption is clearly indicated within Corporations Canada's database; or the fact that information on individuals with significant control available in Corporations Canada's database is about persons who are not captured under beneficial ownership information requirements, or vice versa.

What do we do? When we identify a material discrepancy between the beneficial ownership information of a high-risk corporation incorporated under the Canada Business Corporations Act and the individuals with significant control listed in Corporations Canada's database, we will submit a *Beneficial Ownership Discrepancy Report* to Corporations Canada within 30 days after the day on which the discrepancy is identified. To submit a Beneficial Ownership Discrepancy Report, the corporation must have an active status in Corporations Canada's database.

NOTE: *A material discrepancy that is resolved within 30 days after the day on which it is identified is not required to be reported.*

PEPs and HIOs

A *politically exposed person* (PEP) or the *head of an international organization* (HIO) is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. Their access, influence and control 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 and potential targets of criminals who could exploit their public status and use them, knowingly or unknowingly, to carry out money laundering (ML) or terrorist activity financing (TF) offences. Additionally, family members and close associates of PEPs and HIOs are also potential targets to carry out ML or TF offences because they can more easily avoid detection.

Part of knowing our clients is determining whether a person is a *foreign PEP*, a *domestic PEP*, a *HIO*, or a *family member or close associate of one of these people*.

Foreign PEP

CSS undertakes reasonable measures to determine if a person is a **foreign PEP** or their **family member** or **close associate** when: (1) a *business relationship (BR)* is established, (2) *conducting periodic monitoring based on new facts, situations and risk assessment of our clients' BR*, and (3) *detecting a fact about the existing client BR constitutes reasonable grounds to suspect a PEP/HIO status*.

DEFINITION: A person who holds or has held one of the following offices or positions in or on behalf of a foreign state. These persons are considered foreign PEPs regardless of citizenship, residence status or birthplace.

- 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; or
- Leader or president of a political party represented in a legislature.

Once determined, these persons **are foreign PEPs forever (including deceased foreign PEPs)**. It also includes any prescribed family member of such a person. We treat all clients that we determine to be foreign PEPs or family members or close associates of foreign PEPs as **high-risk**.

Domestic PEP

CSS undertakes reasonable measures to determine if a client is a **domestic PEP or a family member or close associate** of one of those persons when: *(1) a business relationship (BR) is established, (2) conducting periodic monitoring based on new facts, situations and risk assessment of our clients' BR, and (3) detecting a fact about the existing client BR constitutes reasonable grounds to suspect PEP/HIO status.*

DEFINITION: A person who holds, or has held within the last 5 years, a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial government, or a Canadian municipal government:

- Governor General, lieutenant governor or head of government;
- Member of the Senate or House of Commons 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 corporation that is wholly owned directly by His 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; or
- Mayor (head of a city, town, village, or rural or metropolitan municipality, regardless of the size of the population).

A person ceases to be a domestic PEP five years after they have left office or five years after they are deceased. We treat all clients that we determine to be domestic PEPs or family members or close associates of domestic PEPs as **high-risk**.

HIOs

DEFINITION: The *head of an international organization* is a person who is either the head of: (a) an international organization established by the governments of states; or (b) an institution established by an international organization.

An international organization is an organization set up by the governments of more than one country. The key to determining whether you are dealing with a HIO is to determine how the organization was established. If the organization was established by means of a formally signed agreement between the governments of more than one country, then the head of that organization is a HIO. The existence of these organizations is recognized by law in their member countries, but the organizations are not seen to be resident organizations of any one member country (e.g. WHO – World Health Organization; UN - United Nations).

FINTRAC refers to the head of an international organization or the head of an institution established by an international organization as the primary person who leads that organization, for example a president or CEO.

A person **ceases** to be a HIO, five **years** after they are no longer the head of the organization or institution or five years after they are deceased. As with PEPs, CSS treats all clients that we determine to be an HIO or family members or close associates of the HIO as **high-risk**.

Family Member of a PEP (Foreign or Domestic) or HIO

DEFINITION: If a person is a PEP or HIO, then certain family members are considered PEPs or HIOs under the PCMLTFA and associated Regulations. These family members are:

- their spouse or common-law partner;
- their biological or adoptive child(ren);
- their mother(s) or father(s);
- the mother or father of their spouse or common-law partner; and
- A child of their mother or father (sibling).

Once we determine that a client is *a family member of a **foreign PEP***, they remain a *foreign PEP forever* and we are not required to make this determination again. However, we will continue to mitigate the risks associated with family members of foreign PEPs for as long as they remain clients.

Once we determine that a client is *a family member of a **domestic PEP or HIO***, they remain a *domestic PEP until five years* after the domestic PEP and/or HIO has left office. We will continue to mitigate the risks associated with family members of a domestic PEP or HIO for as long as they remain clients.

Close Associate of a PEP (Foreign or Domestic) or HIO

DEFINITION: A close associate can be a person who is closely connected to a PEP or HIO for personal or business reasons. Examples of a close associate (personal or business) include, but are not limited to, persons who:

- are involved as business partners with, or who beneficially own or control a business with, a PEP or HIO;
- are involved 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; or
- Carry out charitable works closely with a PEP or HIO.

Once we have determined that a client is a close associate of a PEP or HIO, the client will remain a close associate until they move jobs or lose that connection.

POLICY:

CSS will identify PEPs and HIOs in accordance with the Act and its Regulations and at the times designated by each client's Business Relationship requirements set out in both the Policy Manual and the separate Risk Assessment Manual. At any time, when a partner, manager or staff detects a fact about a PEP or HIO, that information will be used in constituting reasonable grounds to suspect that a person is a PEP, HIO, or family member or close associate of a PEP or HIO.

PROCEDURES

Procedures:	ACTIVITY	RESPONSIBILITY
Operations	<ul style="list-style-type: none"> CSS compliance will take reasonable measures to make a business relationship (BR) related PEP, HIO, family member or close associate determination when: a business relationship is formed; conducting periodic monitoring of our business relationships; and a fact is detected about an existing business relationship that indicates a PEP or HIO connection. Within 30 days of entering into a BR or detecting a fact about a PEP/HIO, family member or close associate, <i>reasonable measures</i> will be taken to establish the source of the person's wealth, if applicable. Where the relationship is with a business, the PEP/HIO determination should be with the individual with signing authorization. This can be done by asking the person or referring to open source information about the person. This information will be recorded on the Client Business Relationship Record. All BR records must document the office or position of the PEP/HIO, the date of the PEP/HIO determination and who undertook the determination. 	<p>Compliance Team</p> <p>CSS Partner/Staff assigned to Client's file</p> <p>CSS Partner/Staff assigned to Client's file</p> <p>Affirmed by the Compliance Team</p>

Business Relationships

A CSS/client **business relationship (BR)** arises with all clients when the clients have conducted two or more receipt of fund transactions or one suspicious transactions (or a combination of these) within five years from one another.

POLICY:

CSS will undertake ongoing monitoring of all clients for which a business relationship has been established in accordance with the Act and its Regulations.

CSS has chosen to determine that a business relationship has been established as soon as reasonably practicable following the designated transaction requiring that the client's identity be verified. As a best practice, we will see that this is done within **thirty calendar days of the designated transaction or activity**.

When that BR is created, CSS must determine with the client the purpose and intended nature (PIN) of the business relationship. Specifically, the PIN sets out the types of activities and transactions that will take place between CSS and the client. Some examples include transferring funds or securities, paying or receiving funds on behalf of the client and purchasing or selling business assets or entities.

In addition, CSS will establish a scheduled BR review date that requires the CSS compliance team to review the client's transaction history to:

- detect suspicious transactions that have to be reported;
- confirm the client identification and the PIN of the business relationship is current;
- reassess the PEPs/HIO status of the client;
- reassess the client's level of risk using the CSS Client Risk Assessment Questionnaire (the Client Risk Assessment Questionnaire can be found in the Appendix of the Risk Assessment Manual along with its instructions on how to assign the Risk Level);
- the date on which the review was carried out; and
- include the name of the CSS staff member who carried it out.

If as a result of the re-assessment of the existing risk rating it is changed, then the compliance team will adjust the monitoring timeline requirements. For example, If the new risk assessment score is now 'high' the following enhanced due diligence (EDD) measures have been approved to mitigate this level of client risk:

- Monitor the client on a 12-month rotation;
- Confirm information on the client's occupation and volume of assets;
- Confirm information on the client's source of wealth; and
- Obtain CAMLO or Deputy CAMLO review, in consultation with the engagement partner where appropriate, before continuing or expanding a high-risk business relationship.
- Monitoring and reassessment activities should be documented using Appendix B: Monitoring Record in the CSS Risk Assessment Manual.

NOTE: *The CSS **Risk Assessment Manual** sets out in detail the BR monitoring activities associated with all levels of risk associated with our clients including a discussion of triggering events and risk monitoring activities carried out at all three levels of risk used by the Firm: low, medium and high.*

4. REQUIRED REPORTING POLICY

Background

The PCMLTFA requires that accountant reporting entities submit specific reports to FINTRAC for designated transactions identified under the Act and its associated Regulations. To that end, the following Policy has been approved for the Firm.

TYPES OF TRANSACTIONS THAT REQUIRE REPORTING:

Large Cash Transactions:

A transaction involving \$10,000 Canadian or more received in cash within a 24 hour period. These require submission of a Large Cash Transaction Report (LCTR). Large cash transactions do not need to be reported if they are received from a financial entity or public body. In addition, if an accounting Firm receives two or more cash amounts of less than \$10,000.00 each, that total \$10,000.00 or more they must report a cumulative Large Cash Transaction. The Regulations also require CSS to file an LCTR if the employee or partner knows the transactions were made within 24 hours of each other by or on behalf of the same individual or entity.

NOTE: *CSS restricts cash transactions to a maximum of \$5,000.00 CAD per client in a 24-hour period.*

Virtual Currency Transactions:

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.

NOTE: *CSS currently does not, nor does it intend to, accept virtual currency in any form or for any value.*

Listed Person and Entity Property Reporting:

The PCMLTF Regulations stipulate that accountants are required to report a terrorist, terrorist group, listed person or entity property transaction if there are reasonable grounds to suspect that property in our possession or control is owned by or on behalf of a listed person and/or entity. A listed person or entity has been defined as: a terrorist group under the **Criminal Code Section 83.1**; a person or entity subject of an order or regulation under the **United Nations Act**, the **Special Economic Measures Act**; a foreign state that is the subject of an order or regulation made under the **United Nations Act** or the **Special Economic Measures Act**; and a person who is the subject of an order or regulation made under **Section 4 of the Justice for Victims of Corrupt Foreign Officials Act**.

The CAMLO will submit a *Listed Person and Entity Property Report* (LPEPR) if it is determined that the practice has property in its possession or control that is owned or controlled by or on behalf of a terrorist or terrorist group or a listed person and/or entity. This includes information about any transaction or *proposed* transaction relating to that property.

FINTRAC has defined property as any type of real or personal property in our possession or control, including: any deed or instrument giving title or right to property or giving right to money or goods; cash, money orders, traveler's cheques, or bank accounts; insurance policies; securities; and real estate or other assets. **Any transactions that are known to involve terrorist property should not be completed as it is frozen under the Criminal Code.**

Completed Suspicious Transactions:

These are financial transactions that you have reasonable grounds to suspect are related to a completed commission of a money laundering offence or of a terrorist activity financing offence.

Attempted Suspicious Transactions:

These are financial transactions that you have reasonable grounds to suspect are related to the **attempted commission** of a money laundering offence or of a terrorist activity financing offence.

Sanctions Evasion-Related Transactions:

Transactions where there are reasonable grounds to suspect that they are related to sanction evasion by someone acting on behalf of a sanctioned person (this relates to transactions that are both attempted and completed). This would be an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act.

POLICY:

Crawford Smith & Swallow LLP will comply with the legislated requirement to report the following transactions to FINTRAC: Suspicious (Completed or Attempted) Transactions (STR) and Listed Person and Entity Property Reports (LPEPR).

The following sections discuss how CSS manages Suspicious Transactions and Listed Person or Entity Property Reports.

Suspicious Transaction Reporting (Completed and Attempted)

WHAT IS A SUSPICIOUS TRANSACTION?

According to FINTRAC Guidance on Reporting Transactions, **suspicious transactions are those in which there is reasonable grounds to suspect that they are related to the commission or attempted commission of a money laundering or terrorist financing offence.** The PCMLTFA Regulations and the associated guidance are not prescriptive about the factors that may lead someone to deem a transaction, *completed or attempted*, suspicious over another because they may vary from sector to sector and reporting entity to reporting entity.

Consequently, the international consensus has required, particularly the Financial Action Task Force (FATF), that reporting entities need to develop a list of sector specific indicators that together or individually raise questions or concerns about the legitimacy or motives of the individual conducting the completed or attempted transaction. FINTRAC advises all reporting entities to evaluate transactions in terms of what seems appropriate and is within normal practices in their particular line of business and based on knowledge of the specific client.

More specifically, FINTRAC has set down in its relevant guidance that, “**...Reasonable grounds to suspect is a step above simple suspicion and is a conclusion you reach based on an assessment of facts, context, and ML/TF indicators associated with the transaction.**”

Examples of **completed suspicious transaction indicators** that could occur with our clients include:

- 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.
- Large and/or rapid movement of funds not commensurate with the client's financial profile.
- Rounded sum transactions atypical of what would be expected from the client.
- Client has no employees, which is unusual for the type of business.
- Client is paying unusual consultant fees to offshore companies.

An **attempted transaction** is one that a potential client intended to conduct and took some form of action to do so. It is different from a simple request for information, such as an enquiry for a fee quote for a certain transaction. It includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either our employee/partner or the client.

Currently, the AML/ATF Training Course prepared and maintained as current by a third-party service provider includes extensive content covering the identification and subsequent reporting of suspicious transactions (complete and attempted). CSS subscribes to that training course on an annual basis, which is available to all employees and partners on a 24/7 basis.

PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	Ensure CSS employees and partners have training on: <ul style="list-style-type: none"> 1. Suspicious (completed or attempted) Transactions, including known accountant suspicious transaction indicators; and 2. Information on record keeping and client identification requirements. 	Compliance Team
	Contact <u>immediately</u> the Compliance Team if suspicious activity or unusual behaviour is detected.	Employees/Partners
	The compliance team will subsequently: <ul style="list-style-type: none"> 1. Investigate the incident and determine whether to file a STR to FINTRAC; 	Compliance Team



	<p>2. Capture all this information in the CSS Unusual Transaction Log;</p> <p>3. Report STR as soon as practicable from detection and retain a copy of the report and FINTRAC acknowledgement in a secure area. <i>(The compliance team shall send the report to FINTRAC as soon as practicable after she has taken measures 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. Those measures include conducting a full assessment and drafting the prescribed and narrative details of the STR.)</i></p> <p>4. In circumstances where an STR is not filed, make sure to document the reason(s) for not filing in the CSS Unusual Transaction Log.</p> <ul style="list-style-type: none">• Ensure that employees and partners understand that they are forbidden from tipping off the client or anyone else about the contents of the submitted STR.• Ensure that the CSS Policy and Procedure Manual is current and representative of the relevant Regulations and FINTRAC Guidance dealing with STRs.• Ensure that employees and partners understand that no criminal or civil proceedings may be brought against them for making a report in good faith concerning a suspicious transaction (completed or attempted).	<p>Compliance Team</p> <p>Compliance Team</p> <p>Compliance Team</p>
	<p>Penalties for Non-Compliance</p> <p>Ensure employees and partners understand that failure to report a suspicious transaction could lead to criminal penalties, including imprisonment, fines, or both, as set out under the PCMLTFA.</p>	<p>Compliance Team</p>



Required Reporting Policy

STR WORKFLOW

1. 	Staff identifies unusual, attempted, or completed activity.
2. 	Staff documents the relevant facts, including: <ul style="list-style-type: none">• Date and time• Client information• Transaction or activity details• Suspicious indicators observed
3. 	Staff escalates immediately to the CAMLO or Deputy CAMLO.
4. 	CAMLO reviews the information and assesses whether there are reasonable grounds to suspect money laundering (ML) or terrorist financing (TF).
5. 	CAMLO determines one of the following: <ul style="list-style-type: none">• STR required• STR not required• Additional information required
6. 	If an STR is required, the CAMLO submits the report as soon as practicable after suspicion is established.
7. 	CSS retains all supporting documentation and records and must not disclose the existence or filing of an STR to the client or any unauthorized person.



IMPORTANT: Tipping off a client is a criminal offence. Do not disclose the existence or filing of an STR to anyone.

Immunity from Prosecution (STRs)

To be successful, the PCMLTFA must be seen as legislation that protects those who do comply in good faith. Consequently, the following policy has been included.

POLICY:

Crawford Smith & Swallow supports the requirement for employees and partners to identify and report all necessary suspicious transactions (completed or attempted) to FINTRAC and as such recognizes that we are protected from all criminal and civil proceedings for doing so in good faith.

Unauthorized Disclosure of Suspicious Transaction Reports (Completed or Attempted)

POLICY:

CSS understands the seriousness of unauthorized disclosure of suspicious transaction reports (tipping-off) and mandates that its employees and partners comply with the Act and refrain from disclosing any information about a submitted suspicious transaction report (completed or attempted) to anyone within the Firm or elsewhere.

Publicly Available Information and STR Submissions

Client risks can arise from a wide variety of sources. According to FINTRAC's Assessment Manual (July 2025 Version), such sources include: "... **Publicly available information includes news releases issued by industry regulators, police and other law enforcement agencies, mainstream news media and other credible sources**".

Should such information surface, the CSS compliance team will look for links with Firm clients and if confirmed will consider doing further investigation to determine if an STR needs to be filed on impacted clients and if that occurs change the client's risk level to **high** and apply all enhanced due diligence practices plus review the clients business relationship within 30 days and modify the BR to reflect the high risk rating.

The publicly available information on the client will be entered into the CSS Unusual Transaction Log including a summary of the research findings carried out. If reasonable grounds to suspect are established then an STR will be filed as soon as practicable and the STR number will be entered in the UTR Log.

If no reasonable grounds to suspect are identified then the incident will not be reported but all rationale for not reporting must be captured in the UTR Log along with the name of the individual undertaking the investigation and the date the decision not to report was made.

Credible Sources Information and STR Submissions

Whenever CSS receives information from police, law enforcement and national security agencies related to money laundering and terrorist financing in the form of a production order, comfort letters alerts and internal referrals, the compliance team will investigate the situation and the clients impacted. The details

will be entered on the firm's UTR Log; assessed whether an STR needs to be filed or not; record all decisions; and subsequently adjust the client's BR to reflect all changes to risk level and subsequent risk mitigation practices.

Listed Person and Entity Property Reports (LPEPR)

A **Listed Person and Entity Property Report** is triggered by knowing that property is owned or controlled by or on behalf of a terrorist or terrorist group and believing that property is owned or controlled by or on behalf of a listed person. If we know that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group or the transaction is related to property owned or controlled by or on behalf of a listed person, we will not complete the transaction.

As described in FINTRAC Guidance 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. Examples of property for the purpose of a Listed Person or Entity Property Report include among others the following:

- Cash
- Monetary Instruments (e.g. cheques, bank drafts or money orders)
- Accounts (e.g. personal or business accounts, RRSPs, TFSAs)
- Securities (e.g. stocks, bonds or mutual funds)
- Real Estate including an instrument that gives title or right to a property (e.g. a deed)
- Insurance policies

The CSS compliance team must submit a Listed Person or Entity Property Report to FINTRAC as dictated under each of the following:

- A terrorist person/group under Canada's the Criminal Code
- A person or entity that is the subject of an order or regulation made under the United Nations Act
- A person or entity that is the subject of an order or regulation made under the Special Economic Measures Act (SEMA)
- A person who is the subject of an order or regulation made under Section 4 of the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)
- A foreign state that is the subject of an order or regulation made under SEMA or the United Nations Act.

Immunity from Prosecution (LPEPR)

Similar to filing Suspicious Transaction Reports no criminal or civil proceedings will be carried out against the Firm or an employee or partner for submitting a *Listed Person or Entity Property Report* to FINTRAC in good faith.

POLICY:

Crawford Smith & Swallow will undertake a Listed Persons and Entities check using the Dow Jones: Risk Center Financial Crime Search software platform to check clients and associated individuals against the listings monitored therein.

These lists include among others both the: the [Public Safety Canada](#) Web site, which maintains information on Listed Terrorist Entities; and the [Global Affairs Canada](#) Web site, which maintains a webpage devoted to Listed Persons.

Public Safety Canada – Current listed Entities - <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx>

Public Safety Canada - Listed Terrorist Entities – this link will provide the updates - <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/cntr-trrrsm/lstd-ntts/index-en.aspx>

Government of Canada – Consolidated CDN Autonomous Sanction List - [Consolidated Canadian Autonomous Sanctions List](#)

Office of Foreign Assets Control – Sanctions List - [Sanctions List Search](#)

United Nations Security Council – Sanction List Materials - [Search | Security Council](#)

PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	Ensure CSS employees and partners have training on:	
	1. Suspicious terrorist/listed person and entity financing (completed or attempted) transactions.	Compliance Team
	2. CSS currently uses the platforms above to check all clients and associated individuals against the various <i>Listed Persons and Entities</i> listings monitored therein. All clients are automatically checked using this data search product whenever they undertake a transaction with the Firm or if Firm employees or partners suspect that a terrorist/listed person and entity financing transaction may have taken place.	Compliance Team
	3. If the search results in a positive finding, record this fact in the Clients file;	Compliance Team
	4. Freeze all funds held in trust with respect to this transaction;	Compliance Team
	5. Prepare an LPEP Report for immediate submission to FINTRAC, the RCMP and CSIS as designated under the legislation; and,	Compliance Team



	6. In addition, prepare and submit an STR to FINTRAC.	Compliance Team
	7. Automatically elevate the client's risk assessment level to High Risk, subject to all EDD activities associated with that level.	Compliance Team

Economic and Trade Sanction Monitoring Restrictions

To avoid penalties, we have taken steps to ensure awareness of and compliance with Canadian-identified economic trade sanction regimes that have extra-territorial reach. In order to comply with this requirement, we have implemented the following practices:

- CSS currently uses the above sanctioned websites to platform to check all clients and associated individuals against the various individual and entity sanction/terrorist lists where and when required under Canadian legislation; and,
- When it comes to economic and trade sanctions, we will avoid all transactions and client business relationships that deal with prohibited parties or countries.

Currently, the Economic Sanction Lists can be found on the Global Affairs Canada website. The CAMLO, or her designate, is tasked with monitoring that website on a monthly basis and informing all staff members and partners when new Sanctions have been added.

Ministerial Directives and transaction restrictions:

The directive is issued by the Minister of Finance. However, FINTRAC will inform reporting entities that a directive has been issued. 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 will 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.

Directives currently in force:

- [February 24, 2024: Russia](#) Updated on March 22, 2025
- [July 25, 2020: Islamic Republic of Iran](#) Updated on July 14, 2025
- [December 9, 2017: Democratic People's Republic of Korea \(DPRK\)](#) Updated on March 22, 2025

FINTRAC will monitor and assess compliance with directives. FINTRAC can issue administrative monetary penalties to address instances of non-compliance, and may also disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance.

5. REQUIRED RECORD KEEPING POLICY

Background

Accountants and accounting firms have record keeping requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. Specifically, CSS must capture certain information and subsequently maintain a record of that information for specific lengths of time. To that end, we have established the following policy.

POLICY:

Crawford Smith & Swallow supports the requirement for employees and partners to keep all required Records and maintain those records for the designated number of years as outlined in the FINTRAC Record Keeping Requirements Guidance for the accounting sector.

Required Records:

CSS records have been divided into two general categories for ease of description and clarity. These have been titled Designated Records and Client Monitoring Records and include the following:

Designated Records:

- Receipt of Funds
- Suspicious Transaction Report (STR)
- Listed Person and Entity Property Report (LPEPR)

CSS has created two ***Receipt of Funds Record Form*** (deposits and trust accounts) that must be filled in every time we receive an amount of \$3,000 or more in funds. That form includes the following fields that need to be filled in:

- date the funds were received;
- if amount is from a person(s) we include their name, address, date of birth and occupation or if from a sole proprietor we list the nature of their principal business;
- if amount is from an entity(s) then we include the entity name, address and nature of its principal business;
- the amount of funds received and the amount of those funds that were paid in cash;
- the method CSS received the funds (e.g., mail, in person, etc.);
- we list the type and amount of each fiat currency involved in the payment plus any exchange rates used and its source if applicable;
- if the funds came from or were deposited to an account(s) then we record the account numbers, the type of account (savings or chequing) and full name of the/each account holder; and
- finally the purpose of the transaction (e.g., funds to be transferred on the clients behalf).



Both FINTRACs **STR** and **LPEPR** Forms must be filled out and submitted as per FINTRACs Guidance and a copy of each submitted Form stored securely by CSS in a designated location that meets the firms privacy requirements.

Client Monitoring Records:

- Client ID Confirmation Records
- Business Relationship Record
- Ongoing Client Monitoring Records
- Third-Party Determination Records
- PEP and HIO Determination Records
- Ministerial Directive Records

The information captured and held in the above records is discussed in the associated narratives found in other sections of this Manual.

NOTE: *CSS does not undertake any virtual currency transactions nor any large cash transactions (singular or cumulative) to require any 3rd-party determination.*

RECORD RETENTION POLICY

CSS records are stored and retained no less than the time periods set out in Table 1 below.

Required Record	Years to be Retained
1. Receipt of Funds Record	At least 5 years from date the Receipt of Funds record was created.
2. Suspicious Transaction Report Record	At least 5 years after the day the STR was submitted.
3. Listed Person & Entity Property Record	At least 5 years after the day the LPEPR was submitted.
4. Business Relationship Records	At least 5 years after the client ceases to have a BR with CSS.
5. Client ID Confirmation Records	At least 5 years after the last transaction that required ID verification.
6. Ongoing Client Monitoring Records	At least 5 years after the client stops doing business with CSS.
7. PEP/HIO Determination Records	At least 5 years after the client stops doing business with CSS.
8. Ministerial Directive records	At least 5 years after the client stops doing business with CSS.

6. PENALTIES FOR NON-COMPLIANCE POLICY

The PCMLTF Regulations impose stiff non-compliance penalties on reporting entities and their employees.

POLICY:

As stated throughout this manual, Crawford Smith & Swallow LLP is committed to upholding all of the aspects of the Act and its accompanying Regulations. We are determined to ensure that all employees and partners adhere to the spirit of the law and its various obligations.

Any individual within the Firm that fails to live up to this standard will be terminated and/or their working Agreement cancelled.

Penalties for Non-compliance

Non-compliance with Part 1 of the *Proceeds of Crime (Money Laundering) Terrorist Financing Act* may result in criminal or administrative penalties. Both *criminal* and *administrative monetary penalties (AMPs)* cannot be issued against the same instances of non-compliance.

ADMINISTRATIVE MONETARY PENALTIES

FINTRAC has legislative authority to issue Administrative Monetary Penalties (“AMPs”) to reporting entities that are in non-compliance with the PCMLTFA and associated Regulations. AMP violations may be classified as minor, serious, or very serious.

Current penalty ranges may include **\$1 to \$40,000 for a minor violation, \$1 to \$4,000,000 for a serious violation, and \$1 to \$20,000,000 for a very serious violation**, subject to the PCMLTFA and applicable Regulations. Where cumulative penalties apply, maximum penalties may also be determined by reference to gross global income or gross global revenue, as applicable.

CSS will maintain awareness of current FINTRAC penalty guidance and update this Manual as required.

CRIMINAL PENALTIES

Criminal penalties may also apply in certain circumstances, including failures relating to reporting, recordkeeping, client identification, and cooperation with FINTRAC examinations. Criminal penalties may include the following:

- **Failure to report suspicious transactions:** up to \$2 million and/or 5 years imprisonment.
- **Failure to report a large cash transaction or an electronic funds transfer:** up to \$500,000 for the first offence, \$1 million for subsequent offences.
- **Failure to meet record keeping requirements:** up to \$500,000 and/or 5 years imprisonment.
- **Failure to provide assistance or provide information during compliance examination:** up to \$500,000 and/or 5 years imprisonment.



PROCEDURES:

AREA	ACTIVITY	RESPONSIBILITY
Operations	Ensure that all employees, partners, contractors, and other personnel acting on behalf of the Firm receive training with respect to Penalties for non-Compliance with the Act and Regulations.	Compliance Team

7. APPENDICES

APPENDIX A: POSSIBLE ML/TF INDICATORS FOR THE ACCOUNTING SECTOR

CLIENT IDENTIFICATION INDICATORS

- 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 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.

CLIENT BEHAVIOUR INDICATORS

- Client makes statements about involvement in criminal activities.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client exhibits nervous behaviour.
- The client refuses to provide information when required or is reluctant to provide information.
- Client has a defensive stance to questioning.
- Client presents confusing details about the transaction or knows few details about its purpose.



- 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.
- Client makes inquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for source of funds.

CLIENT FINANCIAL CAPACITY INDICATORS

- 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.).
- 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).
- Client appears to be living beyond their means.
- Large and/or rapid movement of funds not commensurate with the client's financial profile.
- Rounded sum transactions atypical of what would be expected from the client.
- Size or type of transactions atypical of what is expected from the client.
- The client's address or employment address are outside the local service area without a reasonable explanation.
- There is a sudden change in client's financial profile, pattern of activity or transactions.

CLIENT BANKING INDICATORS

- Holding multiple accounts at several financial institutions for no apparent reason.
- Suspected use of a personal account for business purposes, or vice versa.
- Client appears 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.
- Use of multiple foreign bank accounts for no apparent reason.
- The same individual(s) holds signing authority for accounts held by multiple entities where there is no legal reason or sufficient explanation for such an arrangement.

CLIENT ATYPICAL TRANSACTION INDICATORS

- Client appears to be structuring amounts to avoid client identification or reporting thresholds.



- Client appears to be collaborating with others to avoid client identification or reporting thresholds.
- Multiple transactions conducted below the reporting threshold within a short time period.
- Client makes inquiries that would indicate a desire to avoid reporting.
- Client exhibits knowledge of reporting thresholds.

CLIENT TRANSACTIONS INVOLVING OTHER COUNTRIES INDICATORS

- 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 Financial Action Task Force.
- Client makes frequent overseas transfers, not in line with their financial profile.

CLIENTS USING THIRD PARTIES

- A client conducts transaction while accompanied, overseen or directed by another party.
- A client makes 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 is linked to seemingly unconnected parties.

TERRORIST FINANCING INDICATORS

- 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, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is 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 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 may be linked to a terrorist organization or terrorist activities.
- 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. crowd funding initiative, charity, NPO, NGO, etc.).

GENERAL ACCOUNTANT CLIENT ML/TF INDICATORS

- 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.
- Client carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Client has no employees, which is unusual for the type of business.
- Client is paying unusual consultant fees to offshore companies.
- Client's records consistently reflect sales at less than cost, thus putting them into a loss position, but they continue without reasonable explanation of the continued loss.
- Client's 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.
- Client makes large payments to subsidiaries or similarly controlled companies that are not within the normal course of business.
- Client 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.
- Client is invoiced by organizations located in a country that does not have adequate ML laws and is known as a highly secretive banking and corporate tax haven.
- An individual asks an accountant to facilitate a financial transaction involving large amounts of
 - cash.
- A client tries to make use of a CSS Trust account when there is no justifiable explanation to support the transaction.
- An individual asks CSS to make a deposit on their behalf which is unusual from their normal business and is not willing to provide additional information.



APPENDIX B: SUGGESTED READING

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations, include:

[The Proceeds of Crime \(Money Laundering\) and Terrorist Financing Suspicious Transaction Reporting Regulations](#)

[The Proceeds of Crime \(Money Laundering\) and Terrorist Financing Regulations](#)

[The Proceeds of Crime \(Money Laundering\) and Terrorist Financing Administrative Monetary Penalties Regulations](#)

FINTRAC NEWS: <https://fintrac-canafe.canada.ca/new-neuf/1-eng>

FINTRAC Compliance program requirements: <https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng>

FINTRAC Risk assessment guidance: <https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/rba/rba-eng>

Reporting suspicious transactions to FINTRAC: <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng.php> and <https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng.php#s4>

FINTRAC assessment manual: The approach and methods used during examinations: <https://fintrac-canafe.canada.ca/guidance-directives/exam-examen/cam/cams-eng>

Department of Finance: Assessment of Money Laundering and Terrorist Financing Risks in Canada (2025): <https://www.canada.ca/en/department-finance/programs/financial-sector-policy/nira-neri/2025.html>

APPENDIX C: GLOSSARY OF TERMS & ABBREVIATIONS

Where a term is defined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), its Regulations, or FINTRAC guidance, the legislative or regulatory definition shall prevail in the event of any inconsistency with this Glossary.

ACCOUNTANTS AND ACCOUNTING FIRMS

Accountants and accounting firms: must fulfill specific obligations as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations to help combat money laundering and terrorist activity financing in Canada. Accountants and accounting firms are subject to the PCMLTFA when they engage in any of the following activities on behalf of a person or entity, or give instructions on behalf of a person or entity in respect of:

- receiving or paying funds or virtual currency;
- purchasing or selling securities, real property or immovables or business assets or entities; or transferring funds, virtual currency or securities by any means.

ADVISORY ENGAGEMENT

A professional engagement in which CSS provides advice, recommendations, planning, consulting, valuation, economic loss quantification, business transition, estate planning, tax planning, or similar professional services without directing or controlling client funds or assets.

AML: Anti-Money Laundering

The framework of laws, regulations, policies, procedures, controls, monitoring, and reporting measures designed to prevent, detect, and deter money laundering.

AML/ATF: Anti-Money Laundering and Anti-Terrorist Financing

The combined compliance framework intended to combat money laundering and terrorist financing.

AMLP: Administrative Monetary Penalty

A monetary penalty that may be imposed by FINTRAC for non-compliance with the PCMLTFA and associated Regulations.

ATF: Anti-Terrorist Financing

Measures designed to prevent the collection, movement, or use of funds for terrorist activities.

AUTO-HIGH RISK OVERRIDE

A risk classification rule requiring automatic assignment of a High-Risk rating when prescribed indicators are present.

BENEFICIAL OWNER

The natural person(s) who ultimately owns, controls, or directs an entity, directly or indirectly. **Beneficial Ownership** requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations apply to all reporting entities (REs). They are the individuals who directly or indirectly own or control 25% 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% or more of the units of the trust. Beneficial owners cannot be other corporations, trusts or other entities. They must be the individuals who are the owners or controllers of the entity.

BENEFICIAL OWNERSHIP INFORMATION

Information obtained regarding individuals who ultimately own or control an entity and the measures taken to verify that information.

BUSINESS RELATIONSHIP

A relationship established between CSS and a client where:

- *FINTRAC-prescribed activities occur; or*
- *an ongoing service relationship exists.*

Business relationships require ongoing monitoring.

CAMLO: Chief Anti-Money Laundering Officer

The individual appointed by CSS with overall responsibility for the AML/ATF Compliance Program.

CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)

Canadian Security Intelligence Service (CSIS) role is to investigate threats, analyze information and produce intelligence. It then reports to, and advises, the Government of Canada to protect the country and its citizens.

CASEWARE

The electronic practice management and engagement documentation system utilized by CSS.

CDD: Customer Due Diligence

Measures taken to identify, verify, understand, and assess a client and the risks associated with the relationship.

CLIENT IDENTIFICATION

Client identification: To verify the identity of a person use the government-issued photo identification method or the dual-process method.

Authentic: In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record.

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.

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.

To verify the identity of an entity use the confirmation of existence method. The record you refer to must be authentic, valid and current.

CLOSE ASSOCIATE

A person closely connected to a PEP or HIO through business, financial, personal, or professional relationships.

COMPLIANCE OFFICER

The individual responsible for overseeing implementation and administration of the AML/ATF Compliance Program.

COMPLIANCE PROGRAM

The AML/ATF framework required by the PCMLTFA consisting of:

- *Appointment of a Compliance Officer;*
- *Written Policies and Procedures;*
- *Risk Assessment;*
- *Ongoing Training Program;*
- *Effectiveness Review;*
- *Ongoing Compliance Monitoring and Controls.*

COMPLIANCE REVIEW

The formal review conducted to assess the effectiveness of the AML/ATF Compliance Program.

CROSS-BORDER CLIENT

A client with foreign residency, foreign operations, foreign ownership, foreign transactions, foreign assets, or other international connections.

CSS: Crawford Smith & Swallow LLP

CSS COMPLIANCE TEAM

The CAMLO, Deputy CAMLO, Partners, and other designated individuals responsible for administering AML/ATF compliance activities.

DEPUTY CAMLO

The individual appointed to support the CAMLO and assume delegated compliance responsibilities.

DOMESTIC PEP

A Politically Exposed Person who currently holds or has held a prescribed prominent public office in Canada.

DUAL PROCESS METHOD

A FINTRAC-approved identity verification method utilizing two independent and reliable sources.

EDD: Enhanced Due Diligence

Additional measures applied to higher-risk clients, transactions, or business relationships.

Examples include:

- *source of wealth review;*
- *source of funds verification;*
- *enhanced monitoring;*
- *management approval;*
- *additional documentation.*
- *Effectiveness Review*

An independent assessment conducted at least once every two years to determine whether the AML/ATF Compliance Program is functioning effectively.

ENGAGEMENT PARTNER

The CSS Partner responsible for oversight of a client relationship or engagement.

ESCALATION EVENT

Any circumstance requiring referral to the CAMLO or Deputy CAMLO.

Examples include:

- *suspicious activity;*
- *sanctions concerns;*

- *PEP/HIO exposure;*
- *unexplained ownership;*
- *refusal to provide information.*

ENTITY

A corporation, trust, partnership, association, organization, estate, or other legal structure.

FAMILY MEMBER (PEP/HIO)

A spouse, common-law partner, parent, child, sibling, or other prescribed family member of a PEP or HIO.

FATF: Financial Action Task Force

Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member countries. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

FINTRAC: Financial Transactions and Reports Analysis Centre of Canada

Canada's financial intelligence unit responsible for administration and enforcement of the PCMLTFA. It was designed to enforce the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its associated Regulations.

FOREIGN PEP

A Politically Exposed Person who currently holds or has held a prescribed prominent public office outside Canada.

FUNDS

Cash, currency, securities, negotiable instruments, virtual currency, or other financial assets.

GUIDELINES/GUIDANCE

Guidelines/Guidance are the plain language interpretation of the *Proceeds of Crime Money Laundering and Terrorist Financing Regulations* (PCMLTFR) and associated requirements that are published by FINTRAC.

HIGH-RISK CLIENT

A client assessed as presenting elevated ML/TF risk requiring Enhanced Due Diligence.

HIGH-RISK JURISDICTION

A country or geographic area identified as presenting elevated money laundering, terrorist financing, sanctions, corruption, or organized crime risk.

HIO: Head of an International Organization

An individual who leads an international organization established by governments.

IFIRM

The client management and workflow system utilized by CSS.

INDEPENDENT REVIEW

A review conducted by a person sufficiently independent of the activities being assessed.

INDIVIDUAL VERIFICATION FORM

The CSS form used to document client identification and identity verification of an individual.

KYC: Know Your Client

The process of identifying, verifying, and understanding a client and the nature of the relationship.

LARGE CASH TRANSACTION REPORT (LCTR)

A report submitted to FINTRAC regarding cash transactions meeting prescribed reporting thresholds.

LISTED PERSON

An individual or entity designated under sanctions, anti-terrorism, or related legislation.

LPEPR: Listed Person or Entity Property Report

Listed Person and Entity Property Reports (LPEPR) is a prescribed transaction that if you have property in your possession or control that you know is owned or controlled by or on behalf of a terrorist or sanctioned individual or group. This includes information about any transaction or proposed transaction relating to that property. This replaces the Terrorist Property Reports.

MEDIUM-RISK CLIENT

A client assessed as presenting moderate ML/TF risk requiring Standard Due Diligence.

ML: Money Laundering

The process of concealing, disguising, converting, transferring, or integrating proceeds derived from criminal activity.

ML/TF: Money Laundering and Terrorist Financing

The combined risks addressed by the AML/ATF regime.

MONITORING RECORD

The CSS document used to document ongoing monitoring activities and reassessment of client risk.

N/A RISK CLASSIFICATION

A classification used where FINTRAC obligations are not triggered and no meaningful ML/TF risk indicators are present.

ONGOING MONITORING

The process of reviewing a business relationship on a continuing basis to:

- *identify changes;*
- *detect unusual activity;*
- *reassess risk;*
- *maintain current information.*

PCMLTFA: Proceeds Of Crime (Money Laundering) and Terrorist Financing Act

Canada's primary AML/ATF legislation. Proceeds of Crime Money Laundering Terrorist Financing Act (PCMLTFA) is designed to help detect and deter money laundering and the financing of terrorist activities. It is also to facilitate investigations and prosecutions of money laundering and terrorist activity financing offences. This includes the reporting, record keeping, client identification and compliance program requirements for accountants and accounting firms.

PEP: Politically Exposed Person

An individual entrusted with a prominent public function in Canada or another country.

PRESCRIBED ACTIVITY

An activity that triggers obligations under the PCMLTFA for accountants and accounting firms.

Examples include:

- *receiving funds;*
- *paying funds;*
- *transferring funds;*

- *purchasing or selling business assets;*
- *purchasing or selling entities;*
- *purchasing or selling securities;*
- *purchasing or selling real property;*
- *dealing in virtual currency where applicable.*

RAM: Risk Assessment Manual

The CSS document used to identify, assess, document, and mitigate ML/TF risks.

RBA: Risk-Based Approach

The FINTRAC methodology requiring compliance measures to be proportionate to identified risk.

REASONABLE MEASURES

Actions taken to obtain, verify, or confirm information as required under the PCMLTFA and Regulations.

ROF: Receipt of Funds Record

The CSS record completed when prescribed funds are received in accordance with AML/ATF requirements.

REPORTING ENTITY

A person or organization subject to obligations under the PCMLTFA.

RESIDUAL RISK

The level of risk remaining after controls and mitigation measures have been implemented.

RISK ASSESSMENT

The process of identifying, measuring, documenting, and mitigating ML/TF risks.

RISK CLASSIFICATION

The final risk rating assigned to a client or business relationship.

Classifications include:

- *N/A*
- *Low Risk*
- *Medium Risk*
- *High Risk*

ROYAL CANADIAN MOUNTED POLICE (RCMP)

Royal Canadian Mounted Police (RCMP) is Canada's national police force.

SANCTIONS

Restrictions imposed under Canadian law against designated individuals, entities, countries, or organizations.

SIMPLIFIED DUE DILIGENCE

Reduced monitoring and documentation measures applied to lower-risk clients where permitted.

SOF: Source of Funds

The origin of money involved in a transaction or relationship.

Examples:

- *salary;*
- *inheritance;*
- *sale of property;*
- *investment proceeds.*

SOW: Source of Wealth

The origin of an individual's total accumulated wealth.

STANDARD DUE DILIGENCE

The normal level of client identification, verification, risk assessment, and monitoring required for medium-risk relationships.

STR: Suspicious Transaction Report

A report submitted to FINTRAC where there are reasonable grounds to suspect a completed or attempted transaction is related to ML/TF. Suspicious Transaction Report (STR) is a report to FINTRAC concerning financial transactions that you have **reasonable grounds to suspect** are related to the commission of a **money laundering/terrorist financing offence**. This includes transactions that you have reasonable grounds to suspect are related to the **attempted** commission of a money laundering offence.

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.

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.

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 the commission of an ML/TF offence.

TF: Terrorist Financing

The collection, provision, movement, or use of funds intended to support terrorist activity or terrorist groups.

THIRD PARTY

A person or entity directing another person or entity to conduct a transaction on their behalf.

THIRD-PARTY DETERMINATION

The process of determining whether a transaction is being conducted on behalf of another person or entity.

TRUST

A legal arrangement in which trustees hold and administer property for beneficiaries.

TRUST ACCOUNT

A bank account maintained by CSS for the receipt, holding, or disbursement of client funds where permitted.

TRIGGER EVENT

An event requiring reassessment of client risk.

Examples include:

- *ownership changes;*
- *unusual transactions;*
- *sanctions concerns;*
- *adverse media;*
- *significant business changes;*
- *PEP/HIO identification.*

UBO: Ultimate Beneficial Owner

The natural person who ultimately owns or controls an entity.

UNKNOWN

- *A response used only where:*
- *information has not yet been obtained;*



- *information cannot reasonably be verified; or*
- *available information is insufficient to support a Yes or No answer.*

Unknown must not be used as a substitute for reasonable inquiry.

U.S. TAX CLIENT

A client with U.S. tax filing obligations, U.S. residency, U.S. citizenship, or significant U.S. tax exposure.

VC: Virtual Currency

A digital representation of value that can be used for payment or investment purposes.

VIRTUAL VERIFICATION

Identity verification conducted without the individual being physically present using FINTRAC-approved methods.

WIRE TRANSFER

An electronic transfer of funds between financial institutions or payment service providers.