Addendum for anti-money laundering legislative changes effective June 1, 2020.

The following sections have been updated to meet the requirement to submit a Suspicious Transaction Report (STR) "**as soon as practicable** after **taking measures to establish there are** Reasonable Grounds to Suspect (RGS) a transaction is related to the commission of a money laundering/terrorist financing offence. "

Part A – Background information

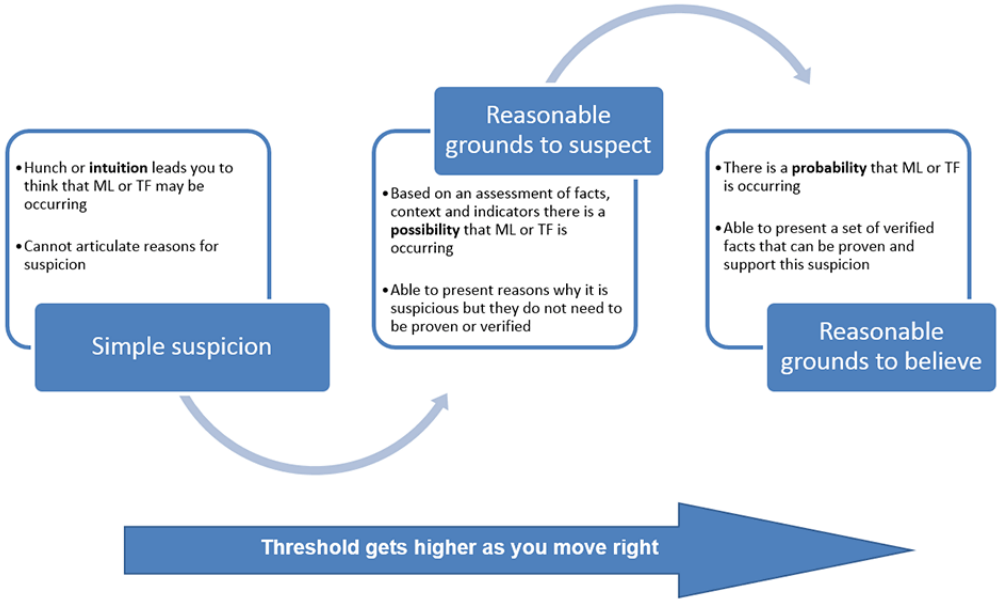
v) Reasonable grounds to suspect

Reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence is the required threshold for reporting a transaction as suspicious.

A financial transaction may not appear suspicious in and of itself. However, additional context about the associated individual or their actions may raise suspicion.

Reasonable grounds to suspect is more than simple suspicion and is a conclusion reached based on an assessment of facts, context and ML/TF indicators associated with the financial transaction. Your suspicion must be reasonable and not biased or prejudiced.

Understanding the differences between the thresholds can help to clarify what reasonable grounds to suspect means and how it can be operationalized within a compliance program. See the diagram below for a visual overview of the following thresholds.



Simple suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a “gut feeling” or “hunch”. Simple suspicion means that you have a feeling that something is unusual or suspicious, but do not have any facts, context or ML/TF indicators to support that feeling or determine if there are reasonable grounds to suspect the occurrence of an ML/TF offence. Simple suspicion could prompt you to assess related financial transactions to see if there are additional facts, context or ML/TF indicators that would support/confirm your suspicion.

Reasonable grounds to suspect is the required threshold for submitting an STR to FINTRAC and is a step above simple suspicion, meaning that there is a **possibility** of an ML/TF offence.

Reaching RGS means that you considered and reviewed the facts, context and ML/TF indicators related to a financial transaction and concluded that there are RGS that this particular financial transaction is related to ML/TF. You must be able to demonstrate and articulate your suspicion of ML/TF in such a way that another individual reviewing the same material with similar knowledge, experience, or training would likely reach the same conclusion.

You **do not** have to verify the facts, context or ML/TF indicators that led to your suspicion, nor do you have to prove that an ML/TF offence has occurred in order to reach RGS.

The explanation of your assessment should be included in the narrative portion, Part G, of the STR. Many factors will support your assessment and conclusion that an ML/TF offence has possibly occurred; they should be included in your report to FINTRAC.

Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is **beyond** what is required to submit an STR. Reasonable grounds to believe means that there are verified facts to support the **probability** that an ML/TF offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe**, **not just suspect**, that ML/TF has occurred. For example, law enforcement must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a production order.

1.2 – Suspicious transactions reporting and record keeping policy

What are suspicious transactions? –FINTRAC’s ‘What is a suspicious transaction report?’ defines suspicious transactions as financial transactions that we have reasonable grounds to suspect are related to the commission of a **money laundering offence or a terrorist activity financing offence**. This includes **attempted** transactions that we have reasonable grounds to suspect are related to

the commission of a money laundering offence or a terrorist activity financing offence.

Requirement – We have to report completed or attempted suspicious transactions to FINTRAC **as soon as practicable after completing the measures required to establish RGS** that a transaction is related to the commission of a money laundering/terrorist financing offence.

As soon as practicable means we have completed the following measures that have allowed us to determine that we have reached the RGS threshold, and therefore **must treat the development and submission of the report as a priority to ensure it is timely**:

- screening for and identifying suspicious transactions;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to the assessment of the facts and context; and
- explaining the grounds for suspicion in an STR, where we articulate how the relevant facts, context and ML/TF indicators allowed us to reach the grounds for suspicion.

In situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, we are encouraged to expedite the submission of STRs. There is no minimum threshold amount for reporting a suspicious transaction. We must make subsequent reports for additional suspicious transactions and periodically re-assess the client to verify that the level of suspicion has not changed.

If we are in receipt of a production order by law enforcement, we must perform an assessment of the facts, context, and ML/TF indicators to determine whether there are RGS that a particular transaction is related to the commission of ML/TF.

Similarly, if we identify a transaction whereby we have reached reasonable grounds to *believe* that an ML/TF offence has occurred, we must begin an assessment of the related transactions immediately as we have *surpassed* the RGS threshold.

Procedures – All employees and associate advisors, if applicable, within this practice are required to bring forward any suspicious transactions to the compliance officer **immediately** once measures have been completed that enabled us to determine there are RGS.

This will enable the compliance officer to develop and submit the suspicious transaction report to FINTRAC as soon as practicable by ensuring the report is timely and unreasonable priority is not given to other tasks. Any delayed reports, should they occur, require a suitable explanation which the compliance officer must keep a record of. The compliance officer files all suspicious transaction reports with

FINTRAC and informs senior management of all suspicious transaction reports. Copies of the submitted reports are retained in a secure location. These records are retained for at least five years from the date the report was submitted.

Confidentiality and immunity
We are not allowed to inform anyone, including the client, about the contents of a suspicious transaction report or even that we have made such a report. This applies whether or not such an investigation has begun.

Since it's important not to tip the client off that we are submitting a suspicious transaction report; we should not be requesting information from the individual conducting or attempting the transaction if we believe that doing so would alert them that a suspicious transaction report is being filed.

No criminal or civil proceedings may be brought against anyone for making a report in good faith concerning a suspicious transaction.

Exception for employees – There is an exception for employees to report, by paper (instead of electronically), directly with FINTRAC in instances where they do not bring forward their suspicion to the compliance officer. Additional information regarding how to submit paper reports can be found in the Paper Reporting section of the "Reporting suspicious transactions to FINTRAC": http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng.asp.

Information to be contained in suspicious transaction report

Consult "Reporting suspicious transactions to FINTRAC": http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide3/str-eng.asp.

All applicable fields in the report including a detailed explanation of what led to the suspicion are completed. Non-mandatory fields on suspicious transaction reports are required to be populated if the information is contained within client files, and if the information was not collected, then in some cases, reasonable measures are required to attempt to get the information. If there is more than one transaction that contributed to the suspicion, include them in the same report.

If available in our client file, additional information will be included in Part G to assist FINTRAC in its analysis and production of financial intelligence disclosures, such as nicknames, beneficial ownership information, IP addresses, additional account numbers, email addresses, and relationships.

Part F – Program review

Use this program for changes after June 1, 2020 – note changes have been made to section: **3) STRs are documented and submitted according to our processes. d)**

Part F – Program review

Policies

A review of policies and procedures must be completed every two years. The compliance officer completes the program review.

Should the practice experience a major change, a program review may be completed before the two-year period has expired. Changes that may trigger an early audit are the purchase of a book of business, legislative/regulatory changes, opening a new office/branch, or noticeable demographic shifts in clientele.

The principal signs the results of the program review within 30 days of completing the review.

Program Review		
Completed by:		**Date**
Results reviewed by:		**Date**
Compliance item reviewed	**Yes/No**	**Results of testing**
1) Appointment of a compliance officer		
Testing includes; a) Ensure a compliance officer has been appointed and approved by senior management	Yes	A compliance officer has been appointed as indicated in the program and the appointment has been approved by the principal as indicated in the compliance officer section of this program.
2) Written compliance policies and procedures are approved, effective and reflect current legislative obligations		
Testing includes: a) Confirm policies and procedures have been approved by the principal.	Yes	Policies and procedures have been approved by the principal as indicated in Part E - Approval and adoption of policies, procedures and training program.
b) Refer to the FINTRAC website to see if there are new legislative changes noted. If there are changes since the date of last review/revisions to this program, make updates as required to ensure program is up to date with FINTRAC guidelines.	Yes	Reviewed website, legislative changes effective 2019 are incorporated in this program.
c) If any reports have been made to FINTRAC ensure appropriate records have been retained.	NA Yes	We have not had any circumstances arise requiring reporting to FINTRAC. We retain a copy of appropriate records related to any reports submitted to FINTRAC.
d) Review the business-based and relationship-based risk assessments to	Yes	Risk assessments include all categories.

ensure that all risk categories have been considered (i.e., geography, products, services, delivery channel and other factors) and that the assessments accurately reflect your current business and client base.		
e) Review all high risks identified in both assessments to ensure risk mitigation measures have been developed and are appropriate to mitigate risk.	Yes	Risk mitigation measures have been documented and implemented.
f) Review 10% of high-risk clients to see if enhanced measures have been conducted i.e., periodic review.	Yes NA	Reviewed 10% of high risk clients, evidence of periodic review was noted. OR At this time there are no high risk clients identified in the practice
g) Confirm enrolment to receive FINTRAC's operational briefs and alerts for more information on ML/TF.	Yes	We are enrolled to receive FINTRAC's operational briefs and alerts.
3) STRs are documented and submitted according to our processes.		
a) Review submitted STRs to determine if similar unreported scenarios exist in book of business.	NA Yes	We do not have STRs at this time. There are no unreported STRs.
b) Review submitted STRS to ensure periodic re-assessment conducted and documented.	NA Yes	We do not have STRs at this time. Periodic re-assessments were conducted and documented as per our procedures
c) Review submitted STRS to ensure all fields populated where information was known.	NA Yes	We do not have STRs at this time. STR fields were completed with the known information.
d) Review measures taken for STRs to reach Reasonable Grounds to Suspect (facts, context and ML/TF indicators) and when these measures were completed (compared to previously submitted transactions, and the complexity, number and nature of the transaction) to ensure the STR was reported as soon as practicable once we met the RGS threshold.	NA Yes	We do not have STRs at this time. STRs were submitted as soon as practicable.
4)Program review has been completed at least every two years and results reviewed		
Testing includes: a)Confirm that a program review has been completed within the	N/A	Implementation of this program replaces the existing program for this practice and as such as program review has not been completed in

past two years	Yes	the past two years. Next program review will be scheduled for two years after implementation of this program or sooner if needed as noted in policies above. OR This program is the first program documented for the practice, a self review will be completed within two years. OR A self review was completed within the past two years, the next self review will be scheduled for two years from implementation of this program.
b) Confirm the review was signed off by the principal.	Yes	The results of this review were signed off as indicated above.
5)Ongoing compliance training – policies and procedures for the frequency and method of training are in place and effective		
Testing includes: a)Ensure frequency of training is detailed in the program.	Yes	The training program states that training will occur annually.
b) Ensure all employees that have exposure to client transactions have received training annually by viewing evidence of training completion.	Yes	Evidence of training maintained and reviewed to ensure that all required employees have received training.
Actions required No actions required at this time.		
Follow-up actions completed		

Other changes to reflect ID requirements such as authentication and to allow for use of electronic images for the dual process method of identifying a client.

3.1 Individuals

Procedures – To ascertain the identity of an individual, we refer to one of two methods. The identity can be ascertained by the advisor or licensed assistant who is contracted with the agency or the insurer.

Single Record Photo ID method

The document must be authentic, valid and current at the time the individual's identity is verified. For example, an **expired** driver's license would **not** be acceptable.

To authenticate a government-issued photo identification document, the original of the physical document, not copies, and its security features will be reviewed in the presence of the client to satisfy that it is authentic as issued by the competent authority (federal, provincial, territorial government), that it is valid (unaltered, not counterfeit) and current (not expired).

The photo-ID document must indicate the individual's name and have a photo of the individual (both of which must match), and have a unique identifier number.

Examples of acceptable photo-ID documents include:

- Driver's license
- Passport
- Permanent resident card
- Citizenship card (issued prior to 2012)
- Certificate of Indian status
- Other similar document issued by a provincial, territorial or federal government

A valid foreign passport may also be acceptable, however, additional records to confirm that the client meets the Canadian residency requirements may be required by the insurer.

When using the photo-ID method, applications and forms are designed to record the following required information:

- The individual's name
- Type of card or document used (e.g. driver's license)
- The unique identifier number on the document or card
- The issuing jurisdiction and country of the document or card (e.g. Alberta, Canada)
- The expiry date, and issue date if available (if the information appears on the card you must record it)
- The date the information was verified

Dual Process Method of Identification

For the dual source method, two valid and current pieces of information are required to be reviewed by the advisor, each from different reliable sources. The individual does not need to be physically present at the time we confirm their identity using this method.

We may use an original record or another version of the information's original format, such as a fax, photocopy, scan, or electronic image.

It is acceptable to use a fax, photocopy, scan or electronic image of a government-issued photo identification document as a source of information.

Each source of information must be used separately to meet one of the following criteria (two out of three categories must be met in total) and we must make sure all the information matches what was provided by the individual:

- Name and address
    - Examples: government-issued photo ID, utility bill or municipality tax statement or CRA notice of assessment
- Name and date of birth
    - Examples: government-issued photo ID, marriage certificate or birth certificate (if no name change)
- Name and financial account (e.g. a deposit, credit card, or loan account)
    - Examples: The most recent financial statement from a securities dealer (not your own firm) or bank account statement

We cannot use the same information or source to satisfy more than one of the categories above. For example, we refer to a CRA notice of assessment to confirm name and address, and a CIBC credit card statement to confirm name and financial account.

Examples of unacceptable identification information:

- Birth or baptismal certificate issued by a church
- Identification card issued by an employer for an employee
- Health card (unless permitted by provincial legislation)

When using the dual process method, applications and forms are designed to record the following required information:

- The individual's name
- The name of the two different sources of information that were used (for example, Canada Revenue Agency, CIBC)
- The type of information (for example, utility statement, bank statement, marriage license, notice of assessment)
- The account or reference number associated with the information
- The date the information was verified.

If we are unable to obtain identification through the sources listed above we consult FINTRAC's Guidance - Know your client - Methods to identify individuals and confirm the existence of entities for additional options.