Anti-Money Laundering & Counter Terrorist Financing (AML/CTF) Training Course

CREA – Module Three

Reporting Requirements

Learning Objectives:

Upon completion of this training module you will be able to:

- State the importance of “know your client” rules as they relate to anti-money laundering and terrorist financing initiatives.
- Identify the reports the real estate industry are required to complete under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PC(ML)TFA).
- Identify when a report must be completed, report completion timeframes, and where reports must be sent.
- State some of the relevant penalties for non-compliance to the PC(ML)TFA.

Fact 1:

Money laundering and terrorist financing is done to obscure the true identity of the individual(s) generating the illicit funds.

Fact 2:

As with any money laundering scheme, it can range from extremely simplistic (the purchasing of property with no attempt to conceal their identity or source of funds) to extremely complicated operations involving offshore transactions, nominees, and lawyers.

Introduction:

- Within the Compliance Regime procedures set out by the PC(ML)TFA Regulations, there are clear reporting requirements for all Canadian **real estate brokers or sales representatives** when they act as an agent in respect of the purchase or sale of real estate.
- Where a real estate broker or sales representative is an employee of a reporting entity, these requirements are the responsibility of the employer except with respect to reporting suspicious or attempted transactions and terrorist property, which is applicable to both.
- Where a real estate agent is acting on behalf of a broker, these requirements are the responsibility of the broker except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.
- These requirements are in place to give FINTRAC the capability **to analyze the reports in order to detect and deter money laundering and terrorist financing activities** within the real estate industry.

In this module, we'll discuss the reporting requirements.

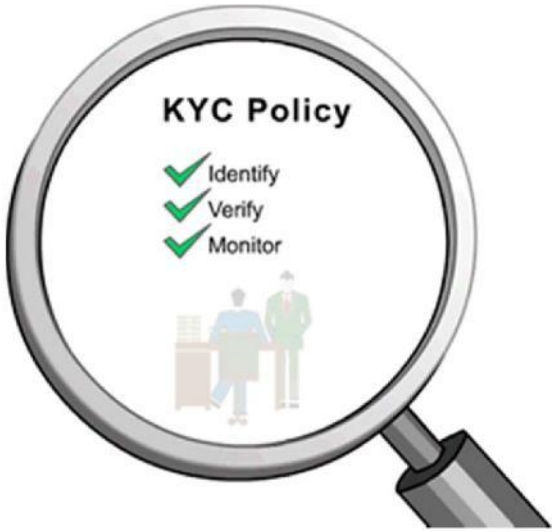
But first, we'll look at the cornerstone to ensuring these reports and records are as accurate and effective as possible; as well as, how a real estate broker or sales representative can take proactive measures towards preventing money laundering or terrorist financing from occurring.

This cornerstone is referred to as **"Know Your Client" or "KYC".**

Mandatory FINTRAC Training 2022

Know Your Client:

KYC Policy:



KYC policy refers to documentation which sets out your company's approach to ensuring that it can effectively **identify, verify and monitor** its clients and the financial transactions in which they engage, relative to the risks of money laundering and terrorism financing.

KYC is important for a number of other reasons. For example, if you know your clients well, you may be able to prevent damage to your company's reputation and avoid fraud, money laundering or excessive risk in financial transactions involving clients.

ROYAL LEPAGE
Team Realty
Independently Owned and Operated, Brokerage

The Principal Objectives of a KYC Policy include:

- ensuring that only legitimate and bona fide clients are accepted;
- ensuring that clients are properly identified and that they understand the risks they may pose;
- verifying the identity of clients using reliable and independent documentation;
- monitoring client accounts and transactions to prevent or detect illegal activities; and
- implementing processes to effectively manage the risks posed by clients trying to misuse your services.

Knowing Your Client is not just Good Business, it is a Regulatory Requirement!

KYC Major Policy Elements:

1. **Client acceptance:** The point at which a new client is accepted or rejected is the easiest point at which the risk of dealing with illegal money can be avoided. By following good client acceptance policies, dealing with entities and individuals who might engage in illegal transactions can be avoided.

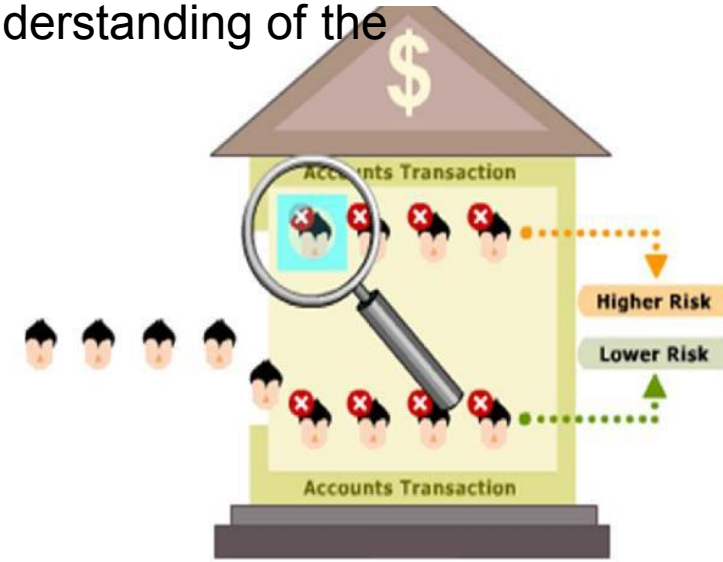
2. **Client identification:** Establishing the identity of clients is central to the KYC policy both for the client acceptance or rejection decision and for the ongoing monitoring of client accounts and transactions. By identifying clients effectively, the business is able to deal with them in the appropriate manner.

3. **Client verification:** Verifying that clients are who they say they are is vital to any client identification procedure. Merely collecting client information is not enough for an effective KYC policy. Reliable and independent documentation should be used to support and confirm the identification details a client provides. For example, citing an original primary photographic identification document such as a passport or driver's licence.

KYC Major Policy Elements continued:

4. **<u>Accounts and transactions monitoring</u>:** In an effective KYC policy, client accounts and transactions are properly classified in terms of risk and are regularly monitored. Through checks and thresholds, unusual activities, activities by high-risk clients, or suspicious behaviour can be detected and reviewed.

5. **<u>Risk management</u>:** To ensure that the risks posed by money laundering and other criminal activities are identified, mitigated and managed good risk management practices are essential. Another objective of the KYC policy is to look past the appearance of the client and obtain visibility into the sources of the client's money. The basic objective is to obtain an understanding of the risk the client poses to business.



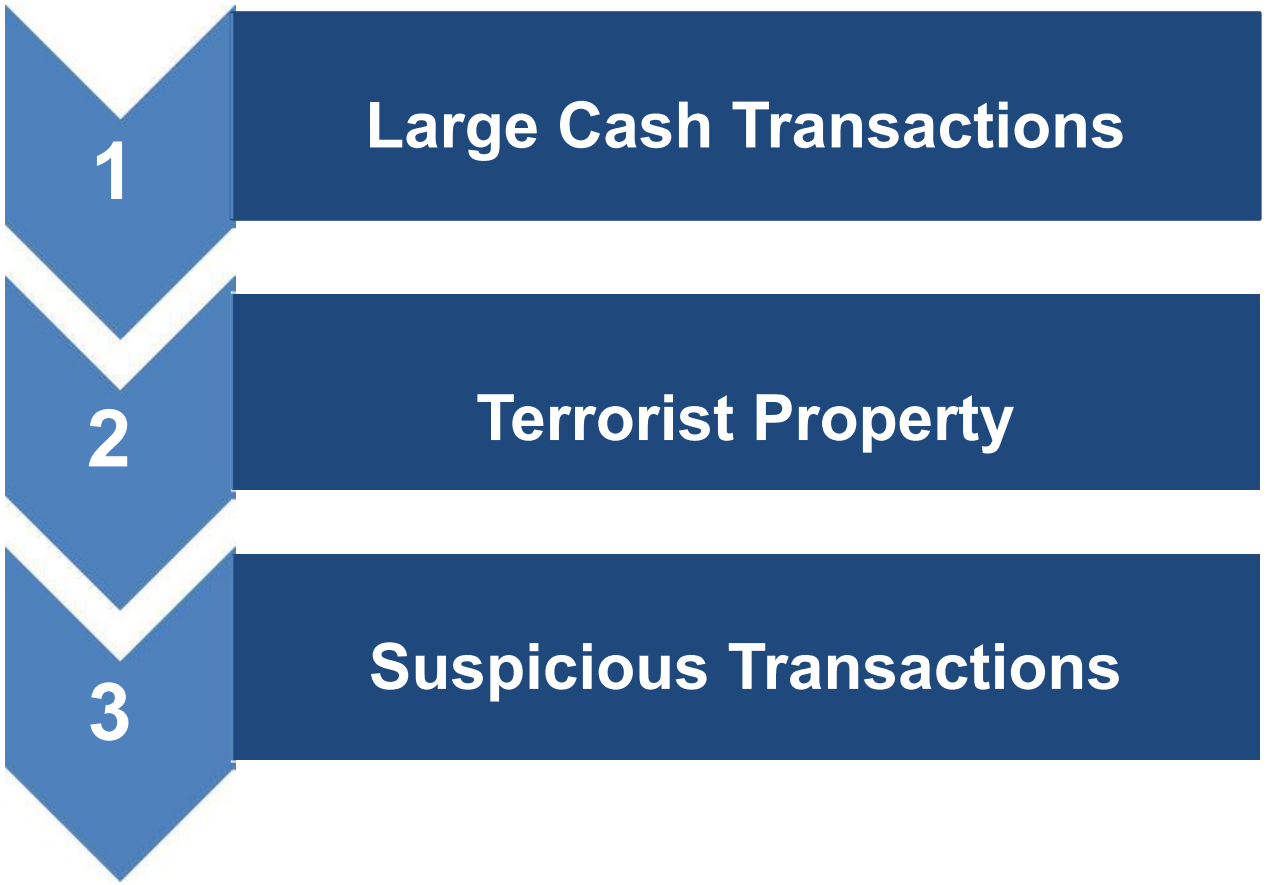
Client Identification:

Taking prudent steps to assess whether the individual you're dealing with is in fact who they say they are can help protect your industry from unknowingly doing business with a criminal or terrorist.

Some of these prudent steps could include:

- Reviewing audited financial statements or annual reports of commercial clients
- Asking for picture identification
- Internet searches
- Visiting the client's office(s)
- Obtaining references

Reporting Obligations:



The Reports

1. Large Cash Transactions

Cash means Canadian currency or foreign currency and includes money in circulation in any country (bank notes or coins) but excludes cheques, money orders or other similar negotiable instruments.

The Reports: 1. Large Cash Transactions

When to Report: A Large Cash Transaction Report must be completed when you:

- Receive an amount of $10,000 CND or more in cash in a single transaction, unless the cash is received from a financial entity or a public body; or

- Undertake two or more cash transactions of less than $10,000 CDN each that together total $10,000 CDN or more within 24 consecutive hours of each other, and are made by or on behalf of the same person or entity.

Foreign Currency: If the transaction is in foreign currency, the funds must be converted into Canadian dollars using the Bank of Canada noon rates available at the time of the transaction. This rate is not based on the exchange rate but only to check whether the funds exceed the $10,000 CDN threshold.

The Reports: 1. Large Cash Transactions

What Does "By or on Behalf of the Same Person" Mean?

1. BY: If an individual, who makes 2 or more transactions, is the same person and the total amount of the transaction is $10,000 or more within 24 consecutive hours, then an LCT Report must be made.

2. ON BEHALF OF: If 2 or more transactions are being made *for* the same person (on behalf of), but the individual is different in each of those transactions, and the amount of the transaction is $10,000 or more an LCT Report must also be made.

The Reports: 1. Large Cash Transactions

Who to Report to and How:

The **report must be sent electronically** to FINTRAC if your company has the capacity to report in that manner.

Please refer to your internal policies and procedures to determine your company's approach for reporting.

Reporting Timeframes:

Large Cash Transaction Reports must be sent to FINTRAC **within 15 calendar days** after the large cash transaction has taken place.

The Reports: 1. Large Cash Transactions

When NOT to Report:

You do **not** have to make a large cash transaction report to FINTRAC:

- If the cash is received from a financial entity. In this context, a financial entity means a bank, credit union, caisse populaire, a trust and loan company or an agent of the Crown that accepts deposit liabilities.
- If the cash is received from a public body. In this context, a public body means any of the following or their agent:
- a provincial or federal department or Crown agency;
- an incorporated municipal body (including an incorporated city, town, village, metropolitan authority, district, county, etc.);
- a hospital authority. A hospital authority means an organization that operates a public hospital.

The Reports: 1. Large Cash Transactions

Penalties for Non-Compliance:

Failure to report a large cash transactions could lead to **criminal charges against those individuals and/or the company** which is subject to the PC(ML)TFA, which upon conviction could result in a fine of up to:

- **$500,000 for the first offence; *and***
- **$1,000,000 for all subsequent offences**.

Administrative monetary penalties (AMPs) are an additional tool to criminal sanctions with the objective of supporting and enhancing efforts to ensure compliance on the part of reporting entities. AMPs allow for a measured and proportionate response to particular instances of non-compliance.

The Reports

2. Terrorist Property

The Reports: 2. Terrorist Property

When to Report: Immediately

A **Terrorist Property Report** must be completed **if you have property in your *possession or control* that you know is owned or controlled by or on behalf of a terrorist or terrorist group or a listed person**. This includes information about any transaction or *proposed* transaction relating to that property.

> **Property means** any type of real or personal property in your possession or control. This includes any deed or instrument giving title or right to property, or giving right to money or goods.
>
> A **terrorist or a terrorist group** includes anyone that has as one of their purposes or activities facilitating or carrying out any terrorist activity. A terrorist group includes anyone on a list published in *Regulations Establishing a List of Entities* issued under the *Criminal Code*.
>
> A **listed person** includes anyone on a list published in the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* issued under the *United Nations Act*.

The Reports: 2. Terrorist Property

Property in these cases can include:

- Cash
- Money orders
- **Real estate**
- Funds in a realtors' trust account

In cases where *you only suspect* that the designated property is owned or controlled by a terrorist or terrorist group, a Suspicious Transaction Report (completed or attempted) should be submitted to FINTRAC.

- When it can be shown that the property belongs to a terrorist and/or terrorist group named on the terrorist lists published by OSFI, then a Terrorist Property Report must be filed with FINTRAC

- In cases, where the terrorist name is similar too, but not an exact match, to a name of a group or individual on the respective OSFI lists then you would file either a Suspicious Transaction (completed or attempted) Report to FINTRAC.

The Reports: 2. Terrorist Property

Who to Report to and How:

The report **must be sent to FINTRAC in paper format** (not electronically) either by registered mail or by fax.

Information in a Terrorist Property Report:

The **Terrorist Property Report** will require information regarding:

- the property
- the suspected terrorist or terrorist group Lists are available on the OSFI website at: http://www.osfi-bsif.gc.ca/osfi/index_e.aspx?ArticleID=2523
- anyone who owns or controls the property on their behalf
- any transactions or proposed transactions related to the property

The Reports: 2. Terrorist Property

Who Else to Report to and How:

In addition to making a **Terrorist Property Report** to FINTRAC, there is also a requirement under the *Criminal Code* to report. It is an offence under the *Criminal Code* to deal with any property if you know that it is owned or controlled by or on behalf of a terrorist or a terrorist group. It is also an offence to be involved in any transactions in respect of such property.

You must disclose to the **RCMP and CSIS**, the existence of property in your possession or control that you know is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about any transaction or proposed transaction relating to that property. Information is to be provided to them, without delay, as follows:

- RCMP, Anti-Terrorist Financing Team, unclassified fax: (613) 949-3113
- CSIS Financing Unit, unclassified fax: (613) 231-0266

A Systemic Approach to Identifying Suspicious Transactions

An effective systemic approach to identify suspicious financial activity may safeguard you and your company from the risk of being involved with terrorist financing and money laundering offences.

Consider the "**SAFE**" approach, which may assist you in meeting the FINTRAC compliance requirements. The four steps of the systemic approach to suspicious activity identification include:

Screen

Ask

Find

Evaluate

Suspicious Activity Identification System

SCREEN - Step 1

Screen the client's account for suspicious indicators

The recognition of an indicator or several indicators of suspicious activity is the first step in the suspicious activity identification system.

ASK – Step 2

Ask the client appropriate questions

If an employee carries out a transaction or transactions for a client bearing one or more suspicious activity indicators then they should question the client on the reason for conducting the transaction and the identity of the source and ultimate beneficiary of the money being transacted.

Suspicious Activity Identification System

FIND - Step 3

Find out from the client's records

Review of information already known when deciding if the apparently suspicious activity is to be expected. In other words - Know Your Client!

EVALUATE – Step 4

Evaluate all the previous information: Is The Transaction Suspicious?

The final step in the suspicious activity identification system is the decision whether or not to complete and submit a **'Suspicious Transaction Report'.**

Such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered.

A reasonable ground to suspect depends on the various suspicious transaction criteria identified for the **real estate industry**.

Examples:

- Client pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Client purchases personal use property under corporate veil when this type of transaction is inconsistent with the ordinary business practice of the client.
- Client purchases property without inspecting it.
- Client purchases multiple properties in a short time period, and seems to have few concerns about the location, condition, and anticipated repair costs, etc. of each property.

Mandatory FINTRAC Training 2022

A reasonable ground to suspect depends on the various suspicious transaction criteria identified for the **real estate industry**.

Examples:

- Client negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference under the table.
- Client pays rent or the amount of a lease in advance using a large amount of cash.
- Client arrives at a real estate closing with a significant amount of cash.
- Client is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided.

Examples:

- Client purchases property in the name of a nominee such as an associate or a relative (other than a spouse).
- Client does not want to put his or her name on any document that would connect him or her with the property or uses different names on Offers to Purchase, closing documents and deposit receipts.
- Client inadequately explains the last minute substitution of the purchasing party's name.
- Client pays initial deposit with a cheque from a third party, other than a spouse or a parent.
- Client sells property below market value with an additional under the table payment.

For additional information about suspicious transactions go to Module 5

Remember that when reporting a suspicious transaction:

- the better you **know your client**, the better position you'll be in to decide whether the transaction is suspicious.
- **transactions or attempted transactions are suspicious**, not people.
- **rarely will one factor alone make a transaction suspicious**.

  Usually, it's a combination of two or more factors that will make a completed transaction or attempted transaction suspicious.

The Reports: 3. Suspicious Transactions (Completed or Attempted)

The Reports

3. Suspicious Transactions

The Reports: 3. Suspicious Transactions (Completed or Attempted)

When to Report: Money Laundering

You must complete a **Suspicious Transaction Report**, once you have **reasonable grounds to suspect** a transaction or attempted transaction is related to a money laundering or a terrorist financing offence.

A reasonable ground to suspect depends on the various suspicious transaction criteria identified for your industry.

Transaction Completion

The Report must be completed regardless if the client completes the financial transaction or attempts a transaction.

The Reports: 3. Suspicious Transactions (Completed or Attempted)

When to Report: Terrorist Financing

Transaction Suspected	The **Suspicious Transaction Report** (completed or attempted) **must be completed** if you **only suspect** that property is owned or controlled by a terrorist or terrorist group.
Transaction Known	If you **know**, rather than suspect, that a transaction or attempted transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, you should **not complete the transaction and fill in a Terrorist Property Report immediately.** This is because terrorist property must be frozen under the *United Nations Suppression of Terrorism Regulations* as well as the Canadian *Criminal Code*.

The Reports: 3. Suspicious Transactions (Completed or Attempted)

Who to Report To and How:

Suspicious Transaction Reports have been developed by FINTRAC and are accessible through their web site. **You must keep a copy of the report for completed or attempted transactions.**

Reporting Timeframes:

A **Suspicious Transaction Report** must be sent to FINTRAC **within 30 calendar days of <u>when you first detected</u> a fact that leads you to have reasonable grounds to suspect** the transaction or attempted transaction is related to a money laundering or terrorist financing offence.

In other words, if it was not until six months later that further client activity made you suspect that possible money laundering or a terrorist financing offence had taken place earlier --- it is from that point six months later that the 30 calendar day reporting time frame begins.

The Reports: 3. Suspicious Transactions (Completed or Attempted)

Tipping Off:

Neither the individual reporting nor the reporting entity may "tip off" anyone by letting them know they made a Suspicious Transaction Report. Therefore, it's important not to ask the client questions that may directly increase their suspicion that the transaction is being considered as abnormal and may be reported to FINTRAC.

Controlling the type of questions asked will assist in protecting the safety of both the individual and the company reporting, as well as any potential criminal investigation.

Your Protection

You are protected from any civil or criminal liability for making a Suspicious Transaction Report **in good faith.**

The Reports: 3. Suspicious Transactions (Completed or Attempted)

Penalties for Non-Compliance:

Failure to report a suspicious transaction could lead to criminal charges against the person and/or entity subject to the PC(ML)TFA, which upon conviction could result in a maximum penalty of:	• **Up to five years imprisonment, *and/or* a** • **Fine of up to $2,000,000**.
Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation:	**up to 2 years imprisonment**.

I'm done Module 3, what do I do now?

Congratulations!

You are now ready to move on to Module 4: Record Keeping and Client Identification.

Good Luck!