Shufti Pro

# KYC Guide Canada

A comprehensive guide to KYC
and AML compliance in Canada

# Table of Contents

# Introduction

As technology has connected beyond traditional barriers of languages and distance, it has created a world of unprecedented economic opportunity. But in doing so it has also significantly increased the risks for doing business both globally and locally. Businesses are under immense regulatory pressure to perform robust customer due diligence, especially to diminish the international threat of money laundering and terror financing. This regulatory pressure manifests itself as Know Your Customer (KYC)[1] regulations and Anti Money Laundering[2] (AML) directives.

Fulfilling KYC and AML requirements is a key focus for obliged enterprises. While these regulations vary from region to region and in some countries, even state to state, major requirements are mainly uniform across the globe and are designed in line with the recommendations of the Financial Action Task Force (FATF).[3] Any organization doing business internationally also needs the agility to meet KYC and AML requirements in a specific region.

This comprehensive guide will provide an overview of how to achieve KYC and AML compliance in Canada.

[1] KYC
[2] AML
[3] FATF

# What is Know Your Customer?

Knowing Your Customer (KYC) in simple words is verifying customers to confirm they are who they claim to be and that they aren't a potential risk to your business.

In this era, where digital evolution is doing wonders and a huge chunk of consumers are online, various industries including but not limited to financial, fintech, e-commerce, real-estate, etc are required to ensure KYC compliance and unfortunately, this is an entirely new activity for many organizations, especially for small businesses and startups, leaving them unsure of how to acquire, assemble and analyze the information correctly.

KYC procedures involve verifying the information that a customer provides and analyzing the risk involved in dealing with certain customers, including the funding sources and business details. Failure to do so brings with it significant risk in terms of financial cost, reputational damage, and potential judiciary consequences

At a minimum, organizations are generally required to verify clients' identity, business type, source of funds and wealth as well as the purpose of specific transactions, and the expected nature and level of transactions.

**There are four primary objectives when gathering KYC information, using a risk-based approach:**

- **Identify the customer**
- **Verify the client's true identity**
- **Understand the customer's activities and source of funding**
- **Monitor the customer's activities regularly**

Verification is performed to check the authenticity of the information provided by the customers. The whole process of verifying identity is very important. It begins with authenticating the user i.e. verification of ID documents. After identity verification, the business checks whether it poses any threat to them. In this way, companies can conduct due diligence, prevent money laundering, and terrorist financing. Since businesses are mostly operating online manual identification is exhausted, cumbersome and in most cases impossible to perform so the financial institutions use an online identity verification.

## Customer Due Diligence (CDD)

Customer Due Diligence (CDD) information comprises the facts about a customer that should enable an organization to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering and terrorist financing. CDD plays a pivotal role in eliminating risks related to money laundering, terrorist financing,[4] fraud, corruption, arms trade, bribery, drug trafficking, and other illegal financial activities.

When opening a customer account according to legal requirements, several checks are required to follow the Know Your Customer procedures. One of the control methods implemented for risk assessment is a sanction, PEP, and adverse media screening.

## What is Anti Money Laundering?

Money laundering is the process of hiding the source of money earned from illicit crimes to circulate it in the financial infrastructure as legal proceeds while manipulating the tax and accountability bodies in the region. **Anti-Money Laundering (AML) refers to rules and regulations implemented to hinder criminals from money laundering. It also includes laws and procedures to identify and counter the financing of terrorism (CFT).**

Money laundering is a serious financial crime and there are global and regional AML regimes to prevent the amalgamation of criminal proceeds in mainstream legal financial systems. Basic AML compliance obligations of the majority of the sectors are similar but the regulations become stricter with the increasing money laundering risk of the entities.

### Do you know?

**According to the report by the B.C. (British Columbia) government's expert panel on money laundering more than $43 billion is laundered in Canada every year and over $3 billion of which is laundered right in Manitoba**[5]

[4] Customer Due Diligence Courses & Know Your Customer Training

[5] Over $3B laundered in province every year according to report

Financial Action Task Force (FATF) provides comprehensive global AML/CFT regulations and policies. The purpose of the establishment of FATF is to build an international standard for the prevention of money laundering. It has 37 member jurisdictions and two regional organizations representing major financial centers in all parts of the globe.


## AML Screening and Monitoring

AML screening and monitoring are some of the basic requirements of a comprehensive AML program. Audits and penalties by the regulators are expected to increase further. The sanctions and PEP lists grow and change regularly. Due to the dynamic nature of these lists, businesses need to scan sanctions, PEPs, and Adverse Media data regularly. The following checklists could be applied for AML screening and Monitoring:

- ### The Risk-based Approach

  In the risk-based approach, the organization performs AML controls according to its risk perception and the risk level of its customers. The risk perception and risk level for each firm and every customer are different. It will be insufficient to apply the same AML controls for every customer. Therefore, organizations should take 2 basic steps for a risk-based approach. The first one is the assessment of the risk and the second is the implementation of the control processes appropriate to the risk levels.

## Enhanced Due DIligence

Enhanced Due Diligence (EDD) is required when a customer is deemed to be at a higher risk than expected. These high-risk customers normally include Politically Exposed Persons (PEPs) or anyone originating from the High-Risk Countries list as outlined by the FATF. EDD measures usually include high monitoring of customers.

The most efficient way to become AML compliant is to conduct thorough customer screening. That being said, it can be difficult and time-consuming to execute these processes consistently at scale. To address these issues, automation plays an increasingly large role in AML compliance.

## Sanction Checks

Sanction checks are special searches from a list of different governmental and international sanction lists to identify individuals or corporations banned from certain activities or sectors. There are thousands of sanction lists globally some of the prominent lists are OFAC[6], FATF[7], PEPs[8]. Financial institutions and businesses should verify that the individual or corporate they are dealing with is not on any of these sanctions and watch lists. The process should be ongoing because sanctions lists are updated regularly.

## Politically Exposed Persons Check

An individual with a high-profile political role or a prominent public function is known as a Politically Exposed Person (PEP). As they have a high position in a country or jurisdiction affairs they are more prone to bribery, corruption, and other offences related to money laundering. This doesn't always mean that they are offenders but to be on the safe side they are declared as high-risk customers. According to FATF, government officials, close family members of these officials, senior executives of state-owned businesses, and leaders of large political parties all come in PEP lists and are considered high-risk[9]. If an enterprise encounters any of these as their customers they should be put in high-risk profiles and must be screened against sanction lists. Moreover, their transactions should be monitored on an ongoing basis.

## Ultimate Beneficial Ownership

The legal beneficiaries of a company whether a corporate or an individual are Ultimate Beneficial Owners (UBOs). Obligated entities have to identify UBOs[10] to prevent money laundering and terrorist financing. People who directly or indirectly own or control 25% or more of a company are generally termed as UBOs. According to FATF, UBOs carry potential ML/TF risks, so financial institutions must verify important information regarding UBOs[11].

[6] OFAC
[7] FATF
[8] PEPs
[9] FATF GUIDANCE
[10] FINTRAC
[11] BEST PRACTICES ON BENEFICIAL OWNERSHIP FOR LEGAL PERSONS

## Adverse Media Screening

Any negative information about the customer or business from various sources in the commercial world is adverse media. These are mostly news covering the individual or a business. It reveals whether a person or a business is involved in any criminal or illegal activities that could affect your organization if you do business with them. This is why it is important to perform adverse media screening.

### Do you know?

**FATF emphasizes adverse media screening of high-risk customers to identify the customer's reputation. (FATF)**

## AML Transaction Monitoring

Monitoring transactions is one of the crucial AML and anti-fraud security processes. Transaction monitoring helps detect suspicious transactions and determine the risk level of transactions carried out by the customers. Financial sectors like Money Services Businesses (MSBs), insurance corporations, financial services, and money transfer companies mediate a large number of financial transactions daily. Transaction screening is one of the crucial AML obligations to detect any suspicious transaction. Ongoing transaction monitoring is necessary to meet AML obligations.

## Suspicious Activity Report

Suspicious Activity Report (SAR) is used to track suspicious activity that will not be flagged in normal monitoring.[12] The main purpose of SAR is to check for illegal activities such as money laundering, terrorist financing, tax evasion, and other financial frauds.

### Do you know?

**In Canada, around 23 million financial transaction reports are submitted annually.[13] FINTRAC received around 235,661 suspicious transaction reports between 2018-19[14]**

[12] Reporting suspicious transactions to FINTRAC
[13] Reporting Suspicion in Canada Insights from the fight against money laundering and terrorist financing
[14] FINTRAC Annual Report 2018–19

## Currency Transaction Report

Currency Transaction Report (CTR) is generated by banks to help prevent money laundering. According to AML laws in most countries, the CTR report is an AML compliance obligation for financial institutions. Banks use CTR to report any bank transaction exceeding $10,000 to relevant regulators.[15] This is a crucial part of AML transaction monitoring failing to report could lead to fines and penalties.


[15] Currency Transaction Report (CTR) - Banking

# Regulations for Businesses Operating in Canada KYC, AML, and Data Privacy

Canada is a founding member of the Financial Action Task Force (FATF) and its KYC and AML regulations are largely consistent with the FATF's standards. The Canadian AML/CFT legislative framework is set out in 'Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)'. This act is placed to facilitate combatting the laundering of illegal proceeds and the financing of terrorist activities.

The mutual evaluation of the Canadian regulatory framework in 2008 found substantial gaps in its implementation of the FATF's 40 recommendations, and as a result, it was subject to annual follow-up reviews. In the country's last evaluation in 2015 - 16, the regulators found several deficiencies, which criminals were exploiting to perform illicit activities in the region. Therefore, the Canadian parliament and authorities made changes to the primary AML regulation (PCMLTFA). The changes were made final in July 2019, with some amendments going into effect immediately, while some came in June 2020, and the majority of them will be implemented in June 2021.[16]

As a result of the amendments, the Canadian organizations have finally received the opportunity to employ remote verification through a photo ID document to broaden their customer base.

[16] Canada Gazette, Part 2, Volume 153, Number 14: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019

Key AML/KYC regulatory authorities in Canada include:

## Proceeds of Crime (Money Laundering) and Terrorist Financing Act

In December 2001, the Proceeds of Crime (Money Laundering) Act was amended to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)[17]. Its objectives include implementing certain measures to detect and prevent money laundering (ML) and terrorist financing (TF) activities, to respond to the threats posed by criminal bodies, and to help in fulfilling the country's internal commitments to participate in the fight against ML and TF.

## FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) – an agency of the government of Canada – was established in 2000 under the Proceeds of Crime (Money Laundering) Act. It is responsible for facilitating the detection, prevention, and deterrence of money laundering, terrorist financing activity, and other threats to the security of Canada.[18]

FINTRAC analyzes and evaluates the reports received from the institutions and intermediaries and discloses suspicions of ML/TF activities to the law enforcement authorities and others permitted by the Act. This helps in facilitating the investigation and prosecution of ML/TF offences.

- ### Know Your Customer

  PCMLTFR specify how and when you must identify an individual or confirm the existence of an organization or an entity other than a corporation[19], to ensure that the information in the identification documents or from other informational sources corresponds to what the individual or a company provided to you.

[17] Proceeds of Crime (Money Laundering) and Terrorist Financing Act
[18] Frequently asked questions (FAQs)
[19] Methods to verify the identity of persons and entities guidance

Verifying the identity of an individual or confirming the existence of a business or an entity other than a corporation will depend on their activities or transactions being carried out. Financial institutions are responsible for identifying clients for activities[20] including account openings and signature card creation, credit card account opening, etc.

PCMLTFR has specified three ways to verify the identity of an individual:

- Government-issued photo identification method*
- Credit file method*
- Dual-process method*

## Government-issued photo identification method

To be used for identity verification of an individual, a government-issued photo identification document must be issued by either a federal, provincial or territorial government. A foreign government-issued photo identification document can be accepted for verification if it is equivalent to a Canadian document. Photo identification documents by municipal governments, Canadian or foreign, are not valid.

For the photo identification method you must record:

- Name of the person
- The date on which you verified the individual's identity
- Type of document used (such as driver's license, passport, etc)
- The unique identifying number of the identity document
- Jurisdiction (province or state) and country that issued the document
- The expiry date of the document (if available)

To determine the authenticity of the document in this method, you can match the characteristics of the original physical document and its security features in the presence of the individual. In case, if the individual is not physically present the authenticity of the document must be checked with the help of a technology capable of evaluating the document's authenticity. And to determine if the individual presenting the document is the same uploading the document, you must conduct a live video session. For instance:

[20] The documents for verification must be authentic, valid and current

- You can ask the individual being verified to send a scanned copy of their document
- Then you can use technology to compare the features of that document against the known security features
- Later you can conduct a live video chat session or ask the individual to take a "selfie" photo to confirm the real identity of the individual

## Credit file method

A credit file document provides a rating of an individual's ability to repay loans. However, companies can request a credit file that does not include a credit assessment, to verify a person's identifying information. TransUnion Canada and Equifax are two bureaus in Canada that provide credit file information for identification purposes.

To be deemed an acceptable method for verification, a credit file must:

- Be issued from a Canadian credit bureau
- Be in existence for at least three years
- Match the name, date of birth, and address with the one provided

Organizations can use an automated system to match the information of their customer or client with the information in their credit files. They can also rely on a third-party vendor (an entity authorized by a Canadian credit bureau to provide access to Canadian credit information) to provide them with the relevant and current information contained in the individual's credit file. If the information provided by your customer doesn't match with the one in the credit file, the credit file method won't be sufficient for customer verification.

For the credit file method you must record:[21]

- Individual's name
- The date you consulted or searched the credit file*
- Name of the Canadian credit bureau or third party vendor holding the credit file
- Individual's credit file number

Companies are also responsible to describe the processes they follow when using the credit file method, and how they will ensure that the information is current and valid.

[21] Methods to verify the identity of persons and entities guidance

## Dual-process method

To verify the identity of the person through the dual-process method, you must refer to any two of the following methods:

- Take information from a reliable source that includes the name and address of the individual
- Take information from a reliable source that includes the name and date of birth of the individual
- Use the information that includes the individual's name and confirms that they have a deposit account, credit card, or other loan accounts with a financial institution

A reliable source is an originator or issuer of information that you trust, and it should be well known and considered reputable.

The information you gather must originate from two different sources and can neither come from the person being verified or from the person or company doing the verification. All of the information mentioned above must match the one provided by the customer.

The information in the categories can be obtained from statements, letters, certificates, forms, or other authentic sources and can be obtained in original form or the form of fax, photocopy, scan, or electronic image.

The same source cannot be used to verify the information in two different categories. For instance, you cannot use a bank statement from Bank A that contains the individual's name and address and another statement from the same bank that contains their name and confirms the existence of a deposit account.

## Anti-money laundering

Under the PCMLTFA[22] and other associated regulations, developing and implementing a sound and comprehensive compliance program is the key factor for fulfilling your record-keeping, reporting, customer identification, and KYC requirements in the country.

There are five essential elements of a compliance program under PCMLTFA, and each one of them is considered to be a pillar of an effective AML/CFT program. These pillars are:

[22] A credit file provides a rating on an individual's ability to repay loans

- Appointing compliance officer responsible for implementing AML program
- Developing and implementing compliance policies and procedures that are kept up-to-date, and include enhanced measures to mitigate high risks
- Risk assessment of your business activities and relationships
- Developing and maintaining an ongoing compliance training program for employees, agents, and others authorized to act on your behalf
- Overall effectiveness review of compliance program (policies, procedures, etc) after every two years

The level of detail and sophistication of your AML program must be according to the size, complexity, structure, and risk of exposure of your organizations to money laundering and terrorist financing.

During a FINTRAC examination of your AML program, it is important to demonstrate that:

- The required documentation is in place, applied, and is regularly updated
- The compliance program is designed to effectively address your company's vulnerability to ML/TF threats
- Employees, compliance agent, and other members authorized are trained accordingly

## Data Privacy

Storing and processing customer data is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA)[23]. This law is enforced by the Office of the Privacy Commissioner of Canada (OPC)[24]. It also governs how private-sector organizations can collect, use, and disclose the personal information of any individual. This act was passed in the late 1990s to promote consumer's trust in electronic commerce. It was also developed to assure other governments that the privacy laws in Canada were strong enough to protect the personal information of citizens of other nationalities.

Under PIPEDA, companies are required to:

- Report to the Canadian Privacy Commissioner regarding security breaches involving personal information
- Notify the individuals affected by data breaches

[23] PIPEDA legislation and related regulations - Office of the Privacy Commissioner of Canada

[24] PIPEDA & the Privacy Act: Data Regulations in Canada

- Keep a record of every security breaches

PIPEDA considers non-compliance as an offence, but unlike GDPR there is no set fine associated with it. Instead, in case of non-compliance, the OPC refers the case to the Attorney General of Canada, for prosecution.

However, the authorities have issued a warning to the companies that fail to report the potential for significant harm could expose them to fines up to $100,000[25] every time an individual is impacted by a security breach.

Another privacy law that came into effect in 1983 and applies to the federal public sector is known as The Privacy Act. It includes around 250 state departments, agencies, and crown organizations.

This act safeguards the privacy rights of Canadian citizens concerning their interactions with the federal government. The Privacy Act applies to the collection, use, disclosure, retention, and disposal of any recorded personal information.

[25] Failure to report Canadian privacy breaches could mean big fines after Nov. 1

# A case of AML compliance failure - Canadian bank fined $1.1 million for failing to report suspicious transactions

In 2016, the federal anti-money laundering agency in Canada, known as Fintrac, levied a $1.15 million[26] penalty against a Canadian bank -- later in 2017 revealed to be Manulife[27] -- for failing to report a suspicious transaction and various money transfers.

The fine was levied against the bank for failing to report:

- Attempted or actual suspicious transaction
- Receipt of $10,000 or more in a single transaction
- An electronic funds transfer of $10,000 or more to a destination outside Canada
- Receipt from outside Canada of an electronic funds transfer of $10,000 or more

The bank was also penalized for failing to apply written compliance policies and procedures that are kept up to date and approved by a senior officer.

## Significant takeaways from this penalty

This penalty is significant for financial institutions because they are reassured that it is important to meet the expectations of their regulatory bodies and that authorities are always ready to promptly address any issues that are identified. In particular, the regulators remain focused on ensuring that:

- Banks dedicate enough resources for KYC and AML compliance.
- Financial institutions should formally document and clearly define the roles and responsibilities for KYC and AML compliance programs.
- They should properly measure the transactions to monitor any suspicious activity and report them timely.

[26] Canadian bank fined $1.1M by anti-money laundering agency

[27] Manulife admits fine by money-laundering watchdog Fintrac

Moreover, the notable amount levied by Fintrac due to the failure to report the suspicious activity is considered as serious as the crime itself. This means that Fintrac considers suspicious transactional activity and the risk of potential financial crime very important. Also, this conduct from Fintrac stresses that the firms need to fix issues identified by the regulators at their earliest. The regulatory body also emphasizes the significance of keeping your books transparent and traceable. Especially the unreported cross-country money transfers put Manulife under punitive fines. So, the organizations need to react fast enough to update automated transaction monitoring and reporting systems, update their written compliance policies and apply them duly.

# Industries requiring to comply with regulations

The process and method for identity verification of clients and customers are the same for every industry that falls under the jurisdiction of FINTRAC. The above-mentioned "know your customer" heading covers every method in detail. But the activities and transactions which require businesses to conduct identification of clients differ for every industry. The following portion will discuss in detail when companies in different industries are required to perform the identity verification process.

## Financial Sector

As a financial institution, every organization is obligated to identify individuals and confirm the existence of entities for certain activities and transactions. Entities can be corporations, partnerships, funds, trusts, and unincorporated organizations or associations.

These activities and transactions are listed below:[28]

- For account openings and creation of signature cards
- For credit card account opening
- Settlors or co-trustees of a trust
- For large cash transactions and suspicious transactions
- Electronic funds transfer worth $1,000 or more
- Foreign currency exchange worth $3,000 or more
- For redeeming or issuing $3,000 or more in traveller's cheques, money orders, or other similar negotiable instruments

While confirming the existence of an entity that is a corporation, financial institutions should also verify its name and address, obtain the beneficial ownership information, and the names of the organizations' directors.

[28] When to verify the identity of persons and entities—Financial entities

### Exceptions

Certain exceptions apply to the activities that are conducted under the domain of the financial sector. Financial institutions are not required to identify an individual or confirm the existence of an entity, when or if:

- You are carrying on activities as a credit card acquiring a business
- The account is opened in the name of an affiliate of a financial entity if that affiliate performs activities similar to those of financial institutions, life insurance companies, agents/brokers, or securities dealers
- Creating a signature card for an account or opening a trust or credit card or account for a public body or a very large organization
- An individual or entity already holds an account with you or authorized to give instructions on an account held with you

## Money Services Businesses (MSB)

Under FINTRAC, an individual or an entity will be considered a money services business (MSB) if they are engaged in the business of:

- Foreign exchange dealing
- Transmitting or remitting funds by any means or through any individual, entity, or electronic funds transfer network
- Issuing or redeeming money orders, traveller's cheques, or other similar negotiable instruments.

As an MSB, you are obligated to identify individuals and confirm the existence of entities for certain activities and transactions. Entities can be corporations, partnerships, funds, trusts, and unincorporated organizations or associations.

These activities and transactions are listed below:[29]

- Client information records

[29] When to verify the identity of persons and entities—Money services businesses and foreign money services businesses

- Issuing or redeeming negotiable instruments worth $3,000 or more
- Remittances or transmissions worth $1,000 or more
- Foreign currency exchange of $3,000 or more
- Large cash transactions
- Suspicious transactions

While confirming the existence of an entity that is a corporation, an MSB should also verify its name and address, obtain the beneficial ownership information, and the names of the organizations' directors.

### Exceptions

Certain exceptions apply to the activities that are conducted under the domain of the money services businesses. MSBs are not required to identify:

- The names of the directors of a corporation that is a securities dealer
- Individuals conducting a large cash transaction if the cash is obtained from a public body or financial entity
- An authorized employee conducting a transaction for their employer under a service agreement
- Individual conducting or attempting to conduct a suspicious transaction only if:
  - You have already identified the person and have no doubts about the identification information
  - You believe that identifying the person would inform them that you are submitting a "Suspicious Transaction Report"

## Real Estate

As a real estate broker, sales representative, or real estate developer you are required to identify individuals and confirm the existence of entities for certain activities and transactions.

These activities and transactions are listed below:[30]

- Receipt of funds
- Client information records
- Large cash transactions worth $10,000 or more in a single transaction or multiple ones within 24 hours
- Suspicious transactions

While confirming the existence of an entity that is a corporation, financial institutions should also verify its name and address, obtain the beneficial ownership information, and the names of the organizations' directors.

In the case of unrepresented parties, each real estate broker or sales official representing a client is responsible to identify them before any business dealings. A real estate developer is considered to be a client or a customer if they hire a broker or sales representative to act as their agent for the sale or purchase of a property. In this situation, the representative must meet the obligations under PCMLTFA and associated regulations. These regulations include identifying the real estate developer that acquired their services.

### Exceptions

As a real estate broker, sales representative, or developer, you do not have to identify an individual or confirm the existence of an entity:

- For the receipt of funds of any amount, only if the amount is received from a public body or financial entity
- When a client information record is kept while conducting transactions for a public body or a very large corporation
- Individual conducting or attempting to conduct a suspicious transaction only if:
  - You have already identified the person and have no doubts about them
  - you believe that identifying the person would alert them that a "Suspicious Transaction Report" is being filed

[30] When to verify the identity of persons and entities — Real estate brokers or sales representatives, and real estate developers

## Insurance sector

As a life insurance company, broker, or independent agent you are required to identify clients and confirm the existence of entities for specific activities and transactions.

The insurance sector companies are responsible to identify their clients:[31]

- Client information records: For the purchase of a life insurance policy or an immediate or deferred annuity worth $10,000 or more throughout the annuity or policy
- Group Plans: When the existence of the plan sponsor is not confirmed or the member's contributions are not made by the sponsor of the plan or by payroll deduction
- Large cash transactions worth $10,000 or more in a single transaction or within 24 hours in case of multiple ones
- Suspicious transactions

### Exceptions

Insurance sector companies are to identify their clients or any entity:

- For purchasing of an exempt policy (a policy issued for insurance protection and not for significant investment purposes)
- For purchasing a group life policy that doesn't provide a savings component or a cash surrender value
- For purchasing of immediate or deferred annuity entirely paid for with the proceeds of a group life insurance policy
- For purchasing a registered annuity policy or retirement income fund

In the case of a group plan, identity verification is not required if the sponsor of the plan (whose existence is already verified and confirmed) has made the contributions for the plan's members or it has been made by payroll deduction.

[31] When to verify the identity of persons and entities — Life insurance companies, brokers and agents

## Gaming

As a Casino or gaming platform, you are required to identify individuals and confirm the existence of entities for certain activities and transactions

These platforms are responsible to identify their clients:[32]

- Account openings and signature card creations
- Extension of credit worth $3,000 or more
- Foreign currency exchange of $3,000 or more
- Remittance or transmission of $1,000 or more
- Suspicious transactions
- Casino disbursements (any payout, whether in cash or not, of $10,000 or more)
- Large cash transactions worth $10,000 or more in a single transaction or within 24 hours in case of multiple ones

In the case of Casino disbursements, every casino is responsible to verify the identities of individuals for:

- Redemption of chips, tokens, or plaques
- Front cash withdrawals
- Safekeeping withdrawals
- Advances on any credit, which include advances by markers or counter cheques
- Payments on bets, which include slot jackpots
- Cashing of cheques or other negotiable instruments
- Reimbursements to clients of travel and entertainment expenses

[32] When to identify individuals and confirm the existence of entities – Casinos

- **Exceptions**

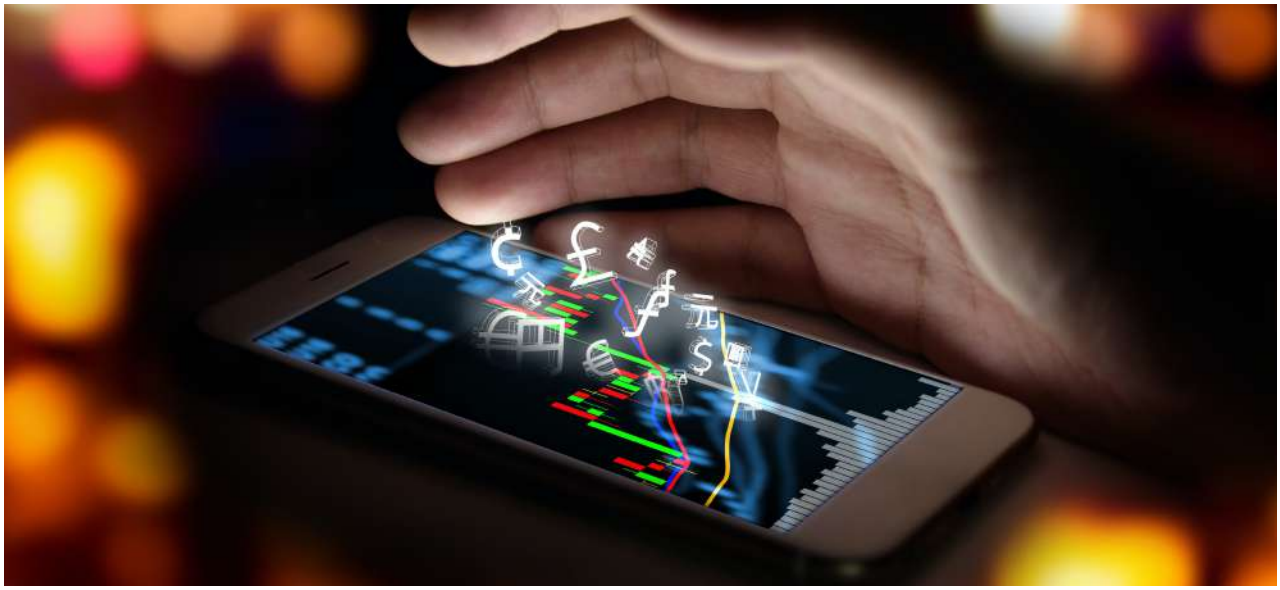
  Casinos or gaming platforms are not required to perform identity verification process while undertaking the following activities for a public body or very large corporation:

  - Open an account
  - Extend credit of more than $3,000 to a client
  - Conduct a foreign currency exchange of $3,000 or more
  - Remit or transmit $1,000 or more
  - Large cash transactions

The same rule goes for the subsidiary of either of those types of entities if the financial statements of the subsidiary are linked with those of the public body or a very large corporation.

## FinTech

There is no single regulator in Canada that oversees the operations of fintech businesses. Rather, this industry may be subject to a variety of laws both federal and provincial, depending on the activities and the regions they operate in.



Securities regulations may apply to fintech businesses that issue securities to the public, along with those that are engaged in activities including Robo advising, crowdfunding, forex trading services, and peer-to-peer lending platforms, among others. FINTRAC is the regulatory authority responsible for overseeing the operations of securities dealers.[33] These dealers or fintech companies -- if they are involved in such activities -- are required to identify clients for:

- Account openings
- Large case transactions
- Suspicious transactions

Other than FINTRAC, federal and provincial privacy laws will also apply to fintech businesses that collect personal information from their customers. PIPEDA governs how fintech companies are permitted to collect, use, and disclose personal data, and what obligations they have to follow in the event of a security breach involving personal customer information under their control.

### Regulatory sandbox programme

The regulatory sandbox programme is implemented by the Canadian Securities Administrators (CSA)[34], to support fintech companies seeking to offer innovative products and services in Canada. This programme allows businesses to register and obtain exemptive relief from requirements of securities laws under a quick and more flexible process as compared to a standard application. This allows them to test their products and services on a time-limited basis in Canada.

## E-Commerce

E-commerce stores in Canada have to follow the regulations in place for verifying the age of customers who want to purchase age-restricted goods online. Selling these products to minors is a major crime. The minimum age for purchasing alcohol in Canada ranges from 18 to 19, depending on the province or territory. The minimum penalty for selling alcohol to a minor is $500. The penalty could reach up to a fine of $10,000, 6 months in jail, or both. These penalties vary for different age-restricted products online.

[33] When to verify the identity of persons and entities—Securities dealers
[34] FinTech Comparative Guide - Technology - Canada

Online retailers should take positive steps to verify the age of the purchaser when selling age-restricted products. Here are some of the checks that are traditionally performed by retailers.

- Relying on the customers to confirm their age
- Using simple disclaimers to make an assumption
- Using an accept statement for the users to confirm that they have read all the terms and conditions and are eligible to purchase their product.
- Accepting payments through credit card without verification that the card belongs to the person making purchases.
- Placing tick boxes to ask customers to confirm that they are of legal age.

## Age verification checks that retailers can adopt

There are a few age verification checks that online retailers can adopt for additional verification:

- Retailers could use age verification checks at the point of delivery by ensuring that delivery drivers request valid proof of age.
- Requiring the customer to provide a valid/acceptable proof of age, which can then be appropriately checked.
- Introduce collect in-store policy. (This strategy may work for some of the retailers having both online and street presence).

Every organization must keep their client data up to date at a frequency that will depend on your risk assessment. As part of ongoing monitoring requirements companies are required to keep all client information updated. Identification information about high-risk clients' must be kept updated as well, with any other appropriate enhanced measures.

For clients that are entities, organizations may consult a paper, electronic record or obtain information verbally to keep the client data up to date.

## Methods to perform KYC and AML

There are various methods to perform KYC and AML that businesses employ for the verification of their customers or clients. Let's discuss a few of the most common methods.

### Private or official databases

Databases are systems that house data previously collected and verified as part of a registration system. They can be private databases run by profit organizations or public databases run by governments. For example, private databases include credit bureaus and telephone directories and public databases include government identifiers (Social Security, tax or voter numbers) or the DMV (Department of motor vehicles) that houses driver's license data and numbers.
While using databases for identity verification, there are certain things that must be considered first including the cost of access, the fact that previous data breaches (if any) may have compromised the credibility of the data, and whether it can be used commercially under current privacy regulations.

### Online verification from ID documents

In online verification, various techniques including artificial intelligence, human intelligence, NFC mobile technology, and facial recognition, are used to determine if a government-issued id document belongs to the user trying to enroll in the system. This method typically requires users to provide a picture of themselves holding an ID document in their hands. By comparing the unique facial features of the live picture with the photo in the ID card we can confirm the

facial similarity and the authenticity of the user. Also, the Shufti Pro NFC verification service is able to scan chip-based identity cards and authenticate your customers with even more speed and accuracy.

Government-issued ID documents might include:

- National identity card
- Driver's license
- Passport
- Residence permit
- Voter identification document
- Tax identification document
- ICAO 9303 Compliant chip-based ID card

There are several ways to evaluate the ID and user, which can help identify possible tampering and impersonation from multiple perspectives:

- **Document template comparison**

  Comparing the submitted ID image against the known document template can identify errors or fake formats. Shufti Pro supports over 3000 document types with 150+ languages.

- **Font anomalies**

  Scammers often try to change fields of data but will leave behind font inconsistencies while doing so.

- **Security features**

  All ID documents have some form of built-in security features like guilloche prints, MRZ, OVI, etc. which while evaluating can ensure authenticity or reveal errors.

To further explain how this method is or can be performed, let's take Shufti Pro -- Identity verification solution -- as an example. Shufti Pro requires the end-user to capture a live picture by showing their face to the camera. Then by using 3D liveness detection, it ensures the presence of the user. After performing all facial checks a facial signature is created which is verified against the image on the document. And being a highly equipped KYC solution it can perform certain other functions as well as anti-spoofing checks, fake image detection, human face attributes analysis, AI mapping techniques, and microexpressions analysis.

## Two-factor authentication (2FA)

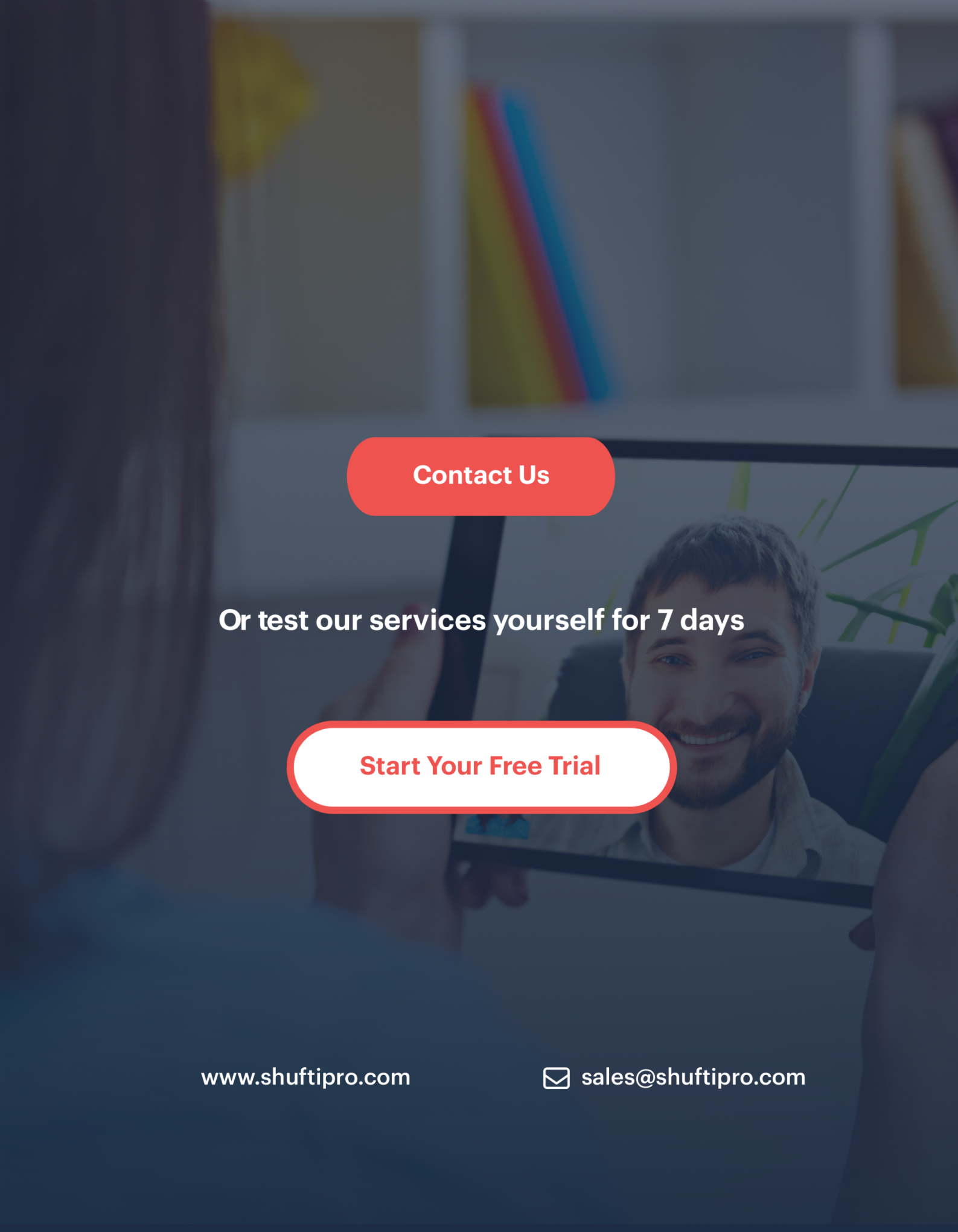
This method requires users to provide a form of personal identification, also known as a token, in addition to the usual username and password details before they can access an account. The token is like a code that can be a number or an alphabet that the user receives from the authenticating agency during the sign-up or login process. 2FA is particularly useful for creating accounts and resetting passwords, however, this method typically requires users to have their cellphones with them during the authentication process. Most identity verification solutions including Shufti Pro offer 2FA as a security feature. It allows businesses to integrate an extra layer of security for customer onboarding and verification.

## Knowledge-Based Authentication (KBA)

KBA verifies a person's identity by requiring an answer to security questions. These questions are generally designed to be easy for the user's to easily remember them. For additional safety, this method allows you to place a requirement for users to answer the questions within a specified time limit. KBA being the easiest verification method for users to understand has a drawback, as it is getting increasingly easy for hackers to discover the answers via social networking sites and other more traditional forms of social engineering.

# Conclusion

To avoid penalties, businesses need to follow KYC and AML laws in Canada. With unprecedented financial growth in every sector, the crime ratio is increasing as well. Hence, the regulatory authorities are increasing the scrutiny to keep bad actors in check. With the availability of technologically advanced verification solutions, KYC and AML compliance operations have now become effortless. These technologies perform verifications in seconds and help in regular monitoring and record-keeping of your customers, and ensure that your business does not fall prey to any criminal activity.



Contact Us

Or test our services yourself for 7 days

Start Your Free Trial

www.shuftipro.com

sales@shuftipro.com

Shufti Pro

Shufti Pro True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.