Viamericas Canada Corporation

AML/ATF Compliance Guide for Agents and Agent Employees

January 2026

AML/ATF Compliance Guide for Agents and Agent Employees - Canada

This AML/ATF Compliance Guide applies to all Agents and Agent Employees supporting business with Viamericas Canada. It has been written to assist in:

- Creating a written Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Compliance Program;
- Designating a Compliance Officer;
- Complying with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, or **PCMLTFA** and its Regulations;
- Safeguarding customer funds and non-public personal information;
- Understanding and adhering to recordkeeping and reporting requirements;
- Conducting an independent review at least annually; and,
- Monitoring, detecting, and reporting suspicious activity.

This AML/ATF Compliance Guide provides a general description of the requirements of the PCMLTFA and how it and other laws relate to your business. Your knowledge of and expertise in the information in this guide may help prevent your business, and Viamericas Canada, from falling victim to crimes such as money laundering and terrorism financing, as well as help your business comply with the law. Further, your agency's compliance with these requirements may help local, provincial, and federal law enforcement agents in their efforts to find and capture those who seek to commit money laundering, terrorist financing, and related crimes and illicit activities.

This guide forms part of Viamericas Canada Corporation's mandatory compliance framework. All agents and agent employees are required to understand and comply with the requirements set out in this guide as a condition of maintaining authorized agent status. Where this guide references obligations imposed by law or by Viamericas Canada policy, those obligations are not optional and must be followed as written. This guide applies to all agency owners, compliance officers, managers, and employees who are involved in, support, or have access to money services business activities conducted on behalf of Viamericas Canada.

It is important to consider that this guide is meant to help your agency and its employees as one part of a complete and effective AML/ATF compliance program. As an Agency Owner, Compliance Officer, and/or Agency Employee, you are tasked with being sure that your business is fully compliant. Failure to comply with the requirements described in this Guide may result in corrective action, including suspension or termination of your agency's relationship with Viamericas Canada.

Contents

Terms Defined

Agent

A business authorized by Viamericas Canada Corporation to provide money transfer or other money services business (MSB) activities on its behalf.

Agent Employee

Any individual employed by, contracted by, or otherwise acting on behalf of an Agent who performs, supports, or has access to MSB activities, systems, customer information, or transaction processing.

Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF)

The body of laws, regulations, policies, and procedures designed to prevent the misuse of financial services for money laundering, terrorist financing, and related criminal activity.

Bank of Canada

Canada's central bank and the federal authority responsible for administering and supervising compliance with the Retail Payment Activities Act (RPAA).

Beneficiary

The individual designated by the Customer to receive funds transmitted through a money transfer transaction.

Close Associate

An individual known to have a close personal, professional, or business relationship with a Politically Exposed Person.

Compliance Officer

The individual designated by an Agent to be responsible for implementing, overseeing, and maintaining the Agent's AML/ATF compliance obligations, including training, recordkeeping, reporting, and cooperation with Viamericas Canada.

Customer (Sender)

An individual who initiates or attempts to initiate a money transfer or other MSB transaction through an Agent on behalf of Viamericas Canada.

Electronic Funds Transfer (EFT)

The transmission of funds through an electronic, digital, or computer-based system, including international money transfers.

FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada, Canada's financial intelligence unit responsible for administering and enforcing compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

Independent Review

An objective assessment of an Agent's AML/ATF compliance program conducted by a qualified individual who does not report to the Compliance Officer and is not involved in day-to-day compliance activities.

Know Your Customer (KYC)

The process of collecting, verifying, and assessing customer identity and related information to understand the nature of customer activity and associated risk. At Viamericas, KYC is often referred to in terms of a KYC Form that must be completed.

Large Cash Transaction Report (LCTR)

A report required under the PCMLTFA for cash transactions totaling $10,000 or more received from or on behalf of the same person within a consecutive 24-hour period.

Listed Person or Entity Property Report (LPEPR)

A report required under the PCMLTFA and the Criminal Code when an entity has property in its possession or control that is owned or controlled by a listed terrorist or terrorist group, or where a transaction involving such a person or entity is attempted or completed.

Ministerial Directives

Binding directions issued by the Minister of Finance of Canada to reporting entities under the PCMLTFA. Ministerial Directives may impose enhanced measures, restrictions, or prohibitions related to transactions involving specified foreign jurisdictions, entities, or activities, and must be followed as issued.

Money Services Business (MSB)

A person or entity engaged in foreign exchange dealing, remitting or transmitting funds, issuing or redeeming money orders or similar instruments, or dealing in virtual currency, as defined under the PCMLTFA.

Non-Public Personal Information (NPPI)

Customer information that is not publicly available and that relates to an individual's identity, financial transactions, or personal details, including identification documents. In Canada, this is governed by **PIPEDA**.

Operational Incident (RPAA)

An event that affects, or could affect, the availability, integrity, confidentiality, or security of systems, funds, or information used to provide payment services.

PIPEDA

Canada's federal privacy law governing the collection, use, and disclosure of non-public personal information in the course of commercial activities.

Politically Exposed Person (PEP)

An individual who holds or has held a prominent public function in Canada or a foreign country, or with an international organization, as defined under Canadian law.

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

Canada's primary federal legislation governing the prevention, detection, and deterrence of money laundering and terrorist financing. The PCMLTFA establishes obligations for money services businesses, including registration, customer identification, recordkeeping, reporting, compliance program requirements, and cooperation with regulatory and law enforcement authorities.

Retail Payment Activities Act (RPAA)

A federal law administered by the Bank of Canada that regulates payment service providers and establishes safeguarding, operational risk, and incident reporting requirements.

Revenu Québec

The provincial authority responsible for administering certain financial compliance obligations in the Province of Québec, including oversight applicable to money services businesses operating in Québec.

Sanctions List

Any list issued or maintained, including under Canadian law, including the United Nations Act, the Special Economic Measures Act, or the Criminal Code, identifying persons or entities subject to sanctions or restrictions.

Structuring

The act of breaking up a transaction or series of transactions into smaller amounts in order to avoid identification, recordkeeping, or reporting requirements.

Suspicious Transaction Report (STR)

A report required under the PCMLTFA when there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering or terrorist financing offence.

Third-Party Transaction

A transaction conducted by a customer on behalf of another person or entity, rather than for the customer's own benefit. Third-party transactions are not permitted.

ViaAcademy

Viamericas Canada's training and learning management platform used to deliver mandatory AML/ATF and operational training to Agents and Agent Employees.

ViaMobi

Viamericas Canada's mobile solution used by Agents to securely submit identification and compliance-related documentation to the Compliance Department.

ViaOne

Viamericas Canada's authorized transaction processing system used by Agents to configure, submit, and manage money transfer transactions.

Money Laundering and Terrorist Financing

Money laundering refers to:

the handling or attempted concealment of funds related to illicit activity.

While money laundering defines a very broad range of activity, for purposes of your work with Viamericas it is important to understand that money transfers are a tool used in money laundering. A person engages in money laundering wherever they know, **or should have known**, that the funds they were touching relate to illicit activity. Understanding how money could be laundered through your business is necessary to identify and prevent such activity.

Money laundering generally involves three stages:

- Placement: the introduction of illicit funds into the financial system, often in the form of cash deposits or other cash-based transactions.
- Layering: the movement, conversion, or transfer of funds through multiple transactions, entities, or jurisdictions to obscure their origin.
- Integration: the re-entry of funds into the economy as seemingly legitimate assets, investments, or financial instruments.

Money services businesses may be used at any stage of this process, including the conversion of cash into electronic transfers and the movement of funds across borders.

Terrorist financing refers simply to:

the processing of funds to sponsor or facilitate terrorist activity.

A terrorist group, like any other criminal organization, seeks to create and maintain a system whereby funds are sourced and channeled to those who facilitate terrorists. Importantly, terrorist financing is not necessarily derived from laundered funds. Funds used for terrorist financing may originate from both illegal and legitimate sources.

Laws like the PCMLTFA were created to fight money laundering, drug trafficking, tax fraud, and possible terrorist financing. To do this, they establish rules that Money Services Businesses (MSBs) must follow.

Structuring

One method of money laundering that is particularly relevant to money transfers is structuring. Many criminals are familiar with transactional thresholds that trigger customer identification, recordkeeping, and reporting requirements. To avoid these thresholds and remain anonymous, criminals may structure their transactions.

Structuring is defined as:

> **the act of breaking up a potentially large transaction into several smaller ones to avoid reporting or recordkeeping requirements.**

It is illegal to structure transactions to avoid these requirements. For example, if a customer attempts to send multiple transactions within a 24-hour period that together exceed a reporting or recordkeeping threshold, this may indicate structuring.

Further, it is also illegal for your agency or any of its employees to assist or aid a customer in structuring transactions to avoid compliance requirements. Specifically, you may not suggest that a customer could avoid providing required information or documentation by conducting smaller transactions. Viamericas Canada Agents and Agent Employees are required to remain alert to structuring indicators and must not assist, encourage, or ignore attempts to avoid compliance requirements.

Some customers may split their transactions with associates or accomplices, including at different times or locations. It is the responsibility of Viamericas Canada Agents and Agent Employees to help identify and prevent this form of money laundering activity.

Examples of structuring may include situations where a customer:

- requests a money transfer and lowers the value after finding out in the process of the transaction that certain identification or documentation is required;
- uses other people to place or receive transactions on their behalf to make the transactions appear unrelated, or to hide that the individual is the true sender or beneficiary; or,
- places transactions on different days, at different agencies, or using different licensed MSB companies to make the transactions appear to be unrelated.

However, not all smaller or multiple transactions are structured transactions. Viamericas Canada Agents and Agent Employees are required to gather the proper information and documentation for such transactions and to escalate concerns where appropriate.

Identifying Suspicious Activity

To prevent money laundering, structuring, and other illicit activity, Viamericas Canada Agents and Agent Employees must be able to detect and identify suspicious activity. However, “suspicious activity” can be difficult to define, as circumstances may vary from customer to customer and transaction to transaction.

For example, one customer’s money transfer transaction to Mexico may be perfectly normal based on your agency’s history with and knowledge of that customer, while another customer’s similar transaction to the same location may be suspicious. The amount, frequency, or other specifics may stand out as suspicious, or the customer’s behavior may appear suspicious. It is important to understand what is both required and recommended to identify and prevent suspicious activities in your business.

Suspicion may arise from completed or attempted transactions, including transactions that are abandoned or not finalized once identification or additional information is requested.

The following are some common examples of what you should consider suspicious activity:

- A customer asks how to avoid a reporting requirement;
- A customer threatens or bribes you to not gather information;
- A customer stops a transaction after you ask for information;
- A customer requests a transaction that is unusually large compared to past transactions, with no apparent explanation;
- A customer provides a fake or altered ID;
- A customer tells you the money he/she is sending comes from illegal activities;
- A customer frequently requests that you exchange small bills for large-denomination bills;
- A customer who regularly conducts transactions but does not appear to reside or work in the area where your agency is located;
- A customer who sends to many different, unrelated beneficiaries; or
- A group of customers who carry out high-value transactions at the same time.

Suspicious activity does not necessarily indicate criminal activity, but it requires further assessment and escalation.

Active Participation and Willful Blindness

Remember: money laundering is a **crime**, and your agency has a responsibility to prevent it.

Active participation in money laundering by your agency is a criminal act. Allowing money laundering to occur when you knew or should have known the transactions relate to illegal activity, known as willful blindness, is equally criminal.

Willful blindness is considered "looking the other way" despite signs that funds used may have come from an illegal activity, that those funds may be laundered, or that the customer is attempting to launder those funds at your agency.

There is no distinction between active participation and willful blindness.

MSBs and Registration

As mentioned, the PCMLTFA and its related regulations require that MSBs fulfill specific compliance obligations.

One such requirement is that MSBs register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

An MSB is an entity conducting business as any of the following (among others):

- Foreign exchange dealing;
- Remitting or transmitting funds (including through any person, entity, or EFT network;
- Issuing or redeeming money orders, traveler's cheques or other similar negotiable instruments, excluding cheques payable to a named person or entity; or,
- Dealing in virtual currency.

Viamericas Canada is an MSB and is therefore required to register with FINTRAC. As part of this requirement, any Viamericas Canada Agent that provides MSB services on its behalf must also be registered with FINTRAC prior to conducting any MSB activity.

Viamericas Canada retains responsibility for FINTRAC registration and for the ongoing maintenance of Agent registration information. Viamericas Canada Agents and Agent Employees are required to provide complete and accurate information and to promptly notify Viamericas Canada of any changes affecting registration status.

If your business provides MSB services on its own, or on behalf of other MSBs, you may also be responsible for separate FINTRAC registration.

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act, and Others

PCMLTFA

The PCMLTFA is a key component of your Agency's compliance regime and where we begin in understanding the roles of Viamericas Canada, your Agency, and each respective employee in identifying and preventing illicit activity.

The PCMLTFA was implemented to establish specific measures for identifying and preventing money laundering and terrorist financing. Some of these measures include:

- establishing recordkeeping and identification requirements for MSBs;
- requiring the reporting of suspicious financial transactions; and,
- establishing a financial intelligence unit (FINTRAC) responsible for collecting, analyzing, and disclosing financial information related to money laundering and terrorist financing.

To read further about the PCMLTFA and the Regulations enacted under it, please visit the FINTRAC website: https://www.fintrac-canafe.gc.ca. For the current consolidated version of the PCMLTFA, see: https://laws-lois.justice.gc.ca/eng/acts/P-24.501/.

Some other important laws, regulations, agencies, and directives include:

Criminal Code
Federal legislation that defines criminal offences in Canada, including offences related to terrorist financing.

FINTRAC
Canada's Financial Intelligence Unit (FIU), responsible for collecting, analyzing, and disclosing financial information under the PCMLTFA.

Ministerial Directives
Binding directives issued by the Minister of Finance under the PCMLTFA that may impose enhanced measures, restrictions, or prohibitions on transactions involving specified jurisdictions, entities, or activities.

Retail Payment Activities Act (RPAA)
In addition to the PCMLTFA, Viamericas Canada is also subject to the Retail Payment Activities Act (RPAA), which establishes federal oversight of retail payment service providers operating in Canada. The RPAA is administered by the Bank of Canada and includes requirements related to operational risk management, safeguarding of end-user funds, and reporting obligations.

Revenu Québec
The provincial authority responsible for administering tax and financial legislation in Québec. Revenu Québec also administers the licensing and oversight regime for MSBs operating in Québec.

Special Economic Measures Act
Authorizes the Government of Canada to impose sanctions, including prohibitions and restrictions, independent of the United Nations Security Council.

United Nations Act

Enables the Government of Canada to implement decisions of the United Nations Security Council (UNSC), including country-specific sanctions measures.

The Retail Payment Activities Act

The Retail Payment Activities Act (RPAA) is a federal law administered by the Bank of Canada that regulates payment service providers, including Viamericas Canada. Agents are not considered PSPs under the RPAA, but because they act on behalf of Viamericas Canada, they must comply with all RPAA-related requirements established by Viamericas Canada. These requirements help ensure the protection of customer funds, the continuity of payment services, and the security of systems and information.

Safeguarding of Funds

Under the RPAA, Viamericas Canada must protect end-user funds. Agents support this obligation by:

- Depositing all collected funds into the designated Viamericas Canada account on the schedule agreed upon.
- Ensuring customer funds are never commingled with the agency's business or personal funds.
- Depositing only into the approved deposit account and never replacing it with another account.
- Avoiding any split or delayed deposits that obscure the true amount collected.

Failure to follow safeguarding procedures may constitute an RPAA operational incident.

Operational Risk Controls

The RPAA requires Viamericas to maintain controls that reduce the likelihood of operational disruptions. Agents must:

- Use only approved systems, devices, and access methods to process transactions.
- Maintain security of systems, passwords, and credentials.
- Ensure the physical and electronic protection of customer information.
- Prevent unauthorized individuals from accessing transaction systems.
- Notify Viamericas Canada immediately if a system, device, or network used to process transactions becomes unavailable, compromised, or malfunctioning.

Agents must follow all operational procedures and technical security requirements issued by Viamericas Canada.

Incident Reporting

The RPAA requires certain incidents to be reported to the Bank of Canada. Agents must notify Viamericas Canada's Compliance Department **immediately** if any of the following occur:

- Loss, theft, unauthorized access, or exposure of customer funds or personal information.
- A system outage, cyber incident, or other disruption affecting transaction processing.
- Errors or delays that prevent timely settlement or release of funds.
- Suspected internal misuse of systems or the Viamericas Canada deposit account.
- Any event that impacts the agent's ability to provide money transfer services.

Viamericas Canada will determine whether a formal RPAA incident report is required. Agents are not responsible for determining whether an incident is reportable to the Bank of Canada. All potential incidents must be escalated to Viamericas Canada for assessment and regulatory reporting, where required.

Recordkeeping for RPAA Compliance

Agents must retain and provide, upon request, all records related to:

- transactions and deposits,
- operational disruptions or system issues,

- customer complaints relating to payment delays or errors, and
- any incident communicated to Viamericas.

Records must be maintained in accordance with Viamericas Canada's instructions and must never be altered or destroyed outside approved retention schedules.

Compliance with Viamericas Canada's RPAA Program

Agents must follow the RPAA policies, procedures, and controls established by Viamericas Canada, including safeguarding requirements, operational risk rules, incident reporting processes, and security practices.

Failure to comply may result in termination of agency status and regulatory consequences for both your business and Viamericas Canada.

The PCMLTFA Compliance Regime

The PCMLTFA requires that each MSB develops and adopts an internal "Compliance Regime" to defend its business against money laundering and terrorist financing. This regime will consist of the following:

- Registration with FINTRAC (as necessary)
- Establish an Effective Written AML Program
- Reporting
- Recordkeeping
- Periodic Independent Reviews
- Initial and Ongoing Training

Each of these components is described in greater detail in the sections that follow and must be implemented together to form an effective Compliance Regime.

The Five Pillars of an AML Program

To establish your Agency's Compliance Regime, Viamericas Canada requires following the "Five Pillars." A complete and effective AML/ATF compliance program is comprised of these five components.

Pillar One: Designate a Compliance Officer

- The officer's responsibilities should include ensuring that:
    - Policies and procedures are followed;
    - Procedures are periodically updated;
    - Employees are properly trained and all training is documented; and
    - Reports are timely and properly filed.

Pillar Two: Tailored Internal Policies, Procedures, and Controls

- Internal policies and procedures should address:
    - Verifying customer identification;
    - Filing reports;
    - Creating and retaining records; and
    - Responding to law enforcement requests.

Pillar Three: Ongoing Training

- The Compliance Officer should ensure employees receive training:
    - Appropriate to their role;
    - Related to employee's responsibilities under the AML/ATF program;
    - Covering the detection and reporting of suspicious transactions; and
    - Upon commencing work and at least annually thereafter.
- The Compliance Officer must prepare and conduct compliance training for all Agency employees (both new and existing), ensuring that all employees receive AML/ATF training at the required intervals.

Pillar Four: Independent Review

- Independent reviews should be carried out by an employee who does not report to the Compliance Officer or a qualified third party, and should address the following issues at a minimum:
    - Availability of the AML/ATF program;
    - Designation of a Compliance Officer;
    - AML training provided to employees;
    - Proper and timely submission of STRs, LCTRs, and other regulatory reports and retention of related documents for 5 years;
    - Compliance with reporting requirements set out in the AML/ATF program; and,
    - Independent reviews may also consider operational or safeguarding requirements under the RPAA.

Pillar Five: Risk and Customer Due Diligence

- Establish the positive identity of your customer, with particular attention to customers or transactions that may represent higher risk.
- The risk assessment identifies and evaluates risks related to products, services, customers, geographic location, and delivery channels.

Pillar One: Designate a Compliance Officer

First, your business should designate a Compliance Officer. The Compliance Officer may be an employee who has other duties at your business, and may even be the Agency Owner, but should be someone in a responsible position.

The Compliance Officer is responsible for your Agency's day-to-day compliance with AML/ATF laws, sanctions requirements, and Viamericas Canada policies. The Compliance Officer is also responsible for ensuring that updates to the compliance program are received, understood, and implemented as required.

The Compliance Officer should additionally be responsible for overseeing your Agency's ongoing compliance training program. Finally, the Compliance Officer should also serve as the point of contact for escalation of suspicious activity.

Pillar Two: Tailored Internal Policies, Procedures, and Controls

As part of an effective compliance regime, your Agency must formally adopt, disclose, and follow a number of policies and procedures as required by law regarding reporting and recordkeeping. The following may serve as a basis for the internal policies, procedures, controls, and reports your Agency is required to manage.

Suspicious Transaction Report

A Suspicious Transaction Report (STR) is a mandatory report that must be prepared in partnership with Viamericas Canada. Transactions determined to be suspicious must be reported to FINTRAC as soon as practicable after the suspicious activity is detected. There is no monetary threshold, and no fixed number of days to report.

An STR must be filed If you know or suspect that a transaction:

- Involves funds derived from illegal activity;
- Is designed to evade PCMLTFA requirements;
- Serves no business or apparent lawful purpose; or
- Involves use of an MSB to facilitate criminal activity.

Viamericas Canada will prepare and submit STRs on your agency's behalf, as well as in its own course of business. However, it is vital to understand the requirements of an STR narrative if Viamericas Canada requests further information. The narrative section of an STR is where you will convey the "story" of what occurred and describe the factors that make a transaction or activity suspicious.

A narrative must include:

- Who performed the suspicious activity, and are any other parties involved?
- What type of money service did the customer use?
- When did the activity take place?
- Where did the activity take place?
- Why do you think the activity was suspicious?
- How did the activity take place?

Large Cash Transaction Report

The Large Cash Transaction Report (LCTR) must be filed with FINTRAC for each transaction where funds are sent or received in cash by the same person in an amount equal to or exceeding $10,000 within any consecutive 24-hour period, whether in a single transaction or multiple transactions.

This report must be filed within fifteen (15) calendar days of the transaction or group of transactions. The $10,000 amount includes both funds sent or received and any related fees.

Viamericas Canada's transactional limits prevent customers from transmitting funds in amounts that would trigger LCTR filing requirements. However, an LCTR may be required where your Agency deposits cash, including in the course of normal business as a Viamericas Canada Agent.

- Name, physical address and phone number;
- Valid identification (including ID type, ID number and place of issuance);
- Date of birth; and,
- Occupation.

The PCMLTFA may require additional reporting when the $10,000/24-hour threshold is reached in connection with other reportable activities, including Third Party Transactions (which are prohibited under the PCMLTFA and Viamericas Canada policy). Viamericas Canada's current transactional limits prevent customers from reaching this threshold.

Recordkeeping

Under FINTRAC guidance, all MSBs must ensure that required sender and beneficiary information accompanies all electronic funds transfers (EFTs) of $1,000 or more. Agents must ensure that sender and beneficiary name, address, city, and postal code (where possible) are entered fully and accurately in ViaOne so that Viamericas Canada can transmit the required data. These requirements form part of the PCMLTFA "Travel Rule," which ensures that required sender and beneficiary information accompanies the EFT.

Your Agency must record certain information for any transaction of $1,000 or more, regardless of the transaction type or method of payment. ViaOne will request this information where required, and it includes:

- Name;
- Physical Address;
- Phone Number;
- Date of Birth;
- ID document;
- Occupation;
- Beneficiary Name;
- Transaction Date and Number; and,
- Transaction Total Amount.

Any physical records created in connection with such transactions must be retained for five (5) years. Further, the PCMLTFA requires that your Agency retain:

- Receipts;
- STRs, LCTRs, and any other reports filed with FINTRAC;
- Any copies of a customer's identification;
- Know Your Customer (KYC) Forms; and,
- A copy of your business-specific AML Compliance Program/Regime.

FINTRAC also requires MSBs to maintain records of attempted suspicious transactions, including incomplete or abandoned transactions, when suspicion is present.

Customer information and related forms must be protected to prevent identity theft and fraud, and to comply with applicable privacy requirements (see "Protecting Privacy").

All documents and records should be organized and readily accessible for internal independent reviews, Viamericas Canada compliance on-site visits, and visits by federal, provincial, and/or local regulators, including FINTRAC.

Records must be maintained in such a way that they can be provided within thirty (30) days of a request to examine them, whether that request is made by Viamericas Canada or FINTRAC. Documents and records may be maintained electronically if a paper copy can be readily produced. Where records are maintained electronically, systems must ensure integrity, accessibility, and retrievability and must allow records to be produced in a readable format upon request.

Transactional Thresholds

Agencies must take reasonable measures to determine whether multiple transactions by the same individual within a 24-hour period are related. Reasonable measures may include reviewing prior-day activity, verifying with other Agency staff, and checking for repeated or patterned transactions.

For transactions exceeding certain limits to or from the same customer in a consecutive 24-hour period (the “24-hour rule”), your Agency must:

- Record and verify the customer’s name, address, and identification document information; and
- Be aware that for certain destination countries, Viamericas Canada may impose stricter identification requirements. ViaOne will prompt that this required information be entered as needed.

Current Viamericas Canada Transactional Limits:

FROM	TO	INTERVAL	THRESHOLD	RANGE
CANADA	ANYWHERE	1 DAY	$1,000 CAD	CAD $1,000 - $2,999.99
CANADA	MX, COL, DR AND HRNC	30 DAYS	$2,000 CAD	CAD $2,000 - $2,999.99
CANADA	ANYWHERE	60 DAYS	Five or more beneficiaries	
CANADA	ANYWHERE	30 DAYS	$3,000 CAD	CAD $3,000 - $9,999
CANADA	ANYWHERE	30 DAYS	$3,000 CAD	CAD $3,000 - $9,999
CANADA	ANYWHERE	180 DAYS	$30,000 CAD	CAD $30,000 - $59,994

For transactions of $999.99 or less, Viamericas Canada requires the following information:

- Full name;
- Full address;
- Telephone number(s);
- Full name of beneficiary;
- City, State and Country information of the beneficiary;
- Beneficiary telephone number;
- Methodology for payment to be received (bank account or cash payout); and,
- If payout is bank deposit, then beneficiary recipient’s financial institution information such as routing number, bank name, and account number.

For transactions of $1,000 to $2,999.99, Viamericas Canada requires:

- Full name;
- Full address;
- Telephone number(s);
- Government Identification Document type and number, and a copy of the ID document;
- Date of birth;
- Occupation;
- Full name of the beneficiary;
- Address details of the beneficiary;
- Beneficiary telephone number;
- How the beneficiary will receive their funds; and,
- The nature of the relationship between the Customer and beneficiary.

For transactions of $3,000 or above, Viamericas Canada requires:

- All the KYC information required for transactions of $1,000 or greater; PLUS
- Name of the Customer's employer;
- Employer's phone number
- Purpose of transaction; and,
- Source of Customer's funds.

If you are required to collect a customer's identification based on these thresholds, the following are common acceptable forms of identification, provided they are valid and current, i.e. have not expired:

- Canadian Military ID;
- Canadian Driver License or ID Card
    - Issued federally or by a province or territory
    - Québec Drivers Licenses may be accepted, but may NOT be requested for identification purposes;
- Foreign-issued Passport or Passport Card;
- Employee Identification
    - Issued federally; and,
- Foreign Government-Issued Identification
    - Examples include the Credencial para Votar (Mexico) and Cedula de Ciudadania (Colombia).

FINTRAC guidance requires that identity be verified using one of the permitted methods: (1) government-issued photo identification, (2) dual-process method, (3) credit file method, or (4) reliable and independent digital sources. Viamericas Canada requires Agents to use the government-issued identification method unless otherwise instructed, and Agents must ensure that identification is valid, authentic, and current.

The identity of a customer must be verified by viewing one of these original, valid identification documents. Although it is not necessary to verify additional information not required above, if you believe information provided by a customer is false, Viamericas Canada recommends that you not complete the transaction.

Customer Identification – Submitting ID Copies

In order to approve and "release" configured transactions, Viamericas Compliance must receive a copy of any identification documents presented. These documents may be submitted to the Viamericas Compliance Department using any of the following methods:

- Barcode Scanner (*preferred*): Scan the barcode on the customer's identification document to automatically populate required fields in ViaOne, reducing errors and processing time.
- ViaMobi: Take a photo using a mobile phone and send it directly to Viamericas Canada's Compliance Department. https://www.viamericas.mobi
- QR Code: Locate the QR code in the customer's ViaOne profile. See training documentation in the ViaOne Resource Center for more information.
- E-mail: If you have a document scanner, scan and send the document to ID@viamericas.com.
- Fax: Documents may be faxed to 1-800-490-8147. Make sure to include the following information for any document:
    - Country of issuance;
    - ID Type;
    - ID Number;
    - Name of the sender as written in the ID;
    - Sender's date of birth; and,
    - ID Expiration Date.

Know Your Customer

The Know Your Customer (KYC) Form helps Agency employees collect required information about a customer. In accordance with the PCMLTFA, the KYC form is required when a customer's transactions exceed certain limits within a given period of time.

KYC requirements align with Viamericas Canada's transactional thresholds and must be completed when identification is required.

The KYC form allows both the Agency and Viamericas Canada to:

- Collect and analyze basic identity information;
- Determine the level of risk posed by a customer;
- Identify transactional patterns; and,
- Monitor a customer's behavior against expected transactional patterns.

The form **must be completed by an Agency employee** using information provided by the customer.

- If your agency uses the "ViaOne" system, you can complete the form directly into the system. The system will then automatically send the form to the Viamericas Compliance Department.
- If your Agency uses the "Red Phone" system, the Call Center Operator will complete the KYC form on your behalf. Before submission, you and the customer must review and sign the completed form.

An example of a Viamericas Canada KYC Form:

Know Your Customer Form
Last revised 10/1/2021

KNOW YOUR CUSTOMER (KYC) FORM
(FORMA CONOZCA A SU CLIENTE)

Date (*Fecha*): ____/____/________ Transaction Number (*Número de Envío*) ____________________

Prepared by (Name) *Preparado por (Nombre)*: ____

Agency Code: _______________ *(Código de la Agencia)* Agency Name: ______________________________ *(Nombre de la Agencia)*

Sender Name: ______________________________________
(Nombre del remitente)

Sender Address (Street, Apartment #, City, Province and Postal Code)
(Dirección del Remitente (incluyendo # de apartamento, ciudad, provincia y código postal)):

____

Sender Telephone: ________________________ *(Teléfono del Remitente)* Type of ID: ______________________________ *(Tipo de identificación)*

ID Number: ______________________________ *(Número del ID)* Issuer Province/Country: ________________________ *(Provincia/País emisor)*

Expiration Date: _____/_____/______ *(Fecha de Expiración)* Date of Birth: _____/_____/______ *(Fecha de nacimiento)*

Beneficiary Name *(Nombre del Beneficiario)*: ______________________________________

Beneficiary Address *(Dirección del Beneficiario)*: ____________________________________

Relationship to Sender *(Relación con el Remitente)*: __________________________________

Amount to Send *(Valor a Enviar)* $______________

Purpose of Transaction *(El dinero será utilizado para)*: __________________________________

Occupation *(Ocupacion)*: ______________________________

I, the Authorized Delegate, certify that I have verified the identity of the client by checking the original, government-issued photo identification document listed herein. I also certify that the information entered accurately reflects the information provided by the client. By clicking on the "Accept and Sign" button, I accept that my name will be the electronic representation of my signature for all relevant purposes.

(Yo, el Representante Autorizado, certifico que he verificado la identidad del cliente al revisar el documento listado arriba. Tambien certifico que la información ingresada refleja la información compartida por el cliente. Al oprimir el botón de "Accept and Sign", acepto que mi nombre servirá como mi firma electrónica para los propósitos relevantes.

____
Authorized Agent's Signature
(Firma del representante de la agencia)

Aggregation Holds and Threshold Reviews

Viamericas Canada may place transactions on hold when a sender or beneficiary reaches or exceeds the above transactional thresholds. These "aggregation" reviews may require additional information, including verification of identity or completion of a short- or long-KYC form.

During an aggregation review, transactions must not be cancelled, refunded, or otherwise released by an Agency until Viamericas Canada's Compliance Department has completed its review. Agents may not bypass an aggregation hold by cancelling and reinitiating transactions.

If additional identity information or KYC documentation is required, ViaOne will automatically notify the customer. Transactions will remain on hold until the Agency submits the requested information or until Compliance determines that the transaction must be cancelled.

Compliance determinations are not shared with Agencies beyond the operational disposition of the transaction. Agencies may contact the Viamericas Canada Compliance Department if there are any questions.

Pillar Three: Ongoing Training

Your Agency should establish an ongoing training program for all parties, including Owners, Compliance Officers, and all Employees who have any involvement in the business's MSB activities. Viamericas Canada recommends that this program be managed by the Compliance Officer.

Training should be thorough and complete, and must include all relevant information contained in this guide prior to any employee conducting MSB-related transactions.

Training should be completed upon onboarding and at least annually thereafter. Completion of training must be documented and retained as part of the Agency's compliance records.

Viamericas Canada provides the ViaAcademy training platform, which offers initial, ongoing, and periodic training tailored to each user's role in the Agency. ViaAcademy and the ViaOne Resource Center each serve as repositories for related training material, including this guide. Employees must complete the assigned training modules and corresponding examinations on the ViaAcademy platform. Successful completion is mandatory to satisfy training requirements.

The ViaAcademy platform, as well as the ViaOne Resource Center, can be accessed through ViaOne.

Pillar Four: Independent Review

Your Agency must conduct and complete an independent review of its AML/ATF compliance regime to assess its effectiveness and adequacy. The frequency and scope of the independent review must be calibrated to the needs and risks of your individual business and adjusted as necessary.

Viamericas Canada requires Agencies to conduct independent reviews at least once per year.

The independent review does not need to be conducted by an outside company and may be performed by a responsible employee of your Agency who does not report to the Compliance Officer. The review may not be conducted by your Agency's Compliance Officer. However, the Compliance Officer is responsible for ensuring that the independent review is completed on schedule.

The independent review should assess the design and operation of the Agency's compliance regime, including policies, procedures, training, reporting, and recordkeeping. Findings from the independent review should be documented and maintained with the Agency's compliance records.

An independent review checklist can be found within the ViaOne Resource Center and in the ViaAcademy document hub. This document may be used for the purpose of completing the review.

Pillar Five: Risk and Customer Due Diligence

The fifth pillar, Risk and Customer Due Diligence, establishes that financial institutions must understand their customers, the transactions they process, and the risks associated with both.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) is a KYC process that provides a greater level of scrutiny of certain customers and their transactions and is designed to highlight risks that may not be identified through standard customer due diligence.

EDD may apply when a transaction appears unusual, inconsistent with expected behavior, or presents elevated or increased risk.

In your agency, you may encounter EDD in the following ways:

- KYC form length: "Short" form vs. "Long" form, assigned depending on customer type or transaction circumstances; and,
- Contact from Viamericas Canada' Compliance Department
  - If information provided does not permit Viamericas Canada to release a transaction, your Agency may be contacted by the Compliance Department to request further information.

List Matches

The name of a sender or beneficiary may match the name of a person included on a restricted list. Restricted lists may include sanctions lists, internal control lists, or other customer restriction lists maintained by Viamericas Canada.

To reduce the likelihood of false positives and ensure accurate screening, Agents should:

- Enter full and complete names for both senders and beneficiaries;
- Enter all surnames and given names where applicable;
- Ensure accurate spelling;
- Enter dates of birth when available; and
- Ensure that customer information entered into ViaOne is accurate and current.

Politically-Exposed Persons and Heads of International Organizations

Viamericas Canada does not permit certain customers to transact due to elevated corruption and financial crime risk. Restricted customer categories include Politically Exposed Persons (PEPs), their Relatives and Close Associates (RCAs), and individuals identified as Heads of International Organizations (HIOs). Customers identified as belonging to any of these categories cannot send or receive transactions through Viamericas Canada.

Identification of PEPs, HIOs, and RCAs is performed by Viamericas Canada's Compliance Department. Compliance determinations are not shared with Agencies beyond the operational disposition of the transaction (for example, whether it must be cancelled).

Politically-Exposed Persons

Under the PCMLTFA, a Politically Exposed Person (PEP) is an individual who is or has been entrusted with prominent public functions by a country or an international organization.

Domestic PEPs include individuals who hold, or who have held within the last five years, specific roles or positions in or on behalf of the federal, provincial (or territorial), or municipal government of Canada.

Foreign PEPs include individuals who hold, or who have held, similar roles in foreign governments.

Viamericas Canada does not permit PEPs to transact.

Relatives and Close Associates

Relatives and Close Associates (RCAs) of PEPs are individuals who are connected to a PEP for familial, personal, or business reasons. RCAs may include spouses, partners, parents, children, siblings, business associates, or similar close connections.

Viamericas Canada does not permit RCAs to transact.

Heads of International Organizations

Heads of International Organizations (HIOs) are individuals who hold senior roles in international organizations that are established by treaty, formal agreement, or that are recognized by multiple governments. Examples may include senior leadership positions within the United Nations, Organization of American States (OAS), Organization for Economic Cooperation and Development (OECD), or similar international bodies.

Viamericas Canada does not permit HIOs to transact.

List Match Reporting

Transactions may be placed on hold when a sender or beneficiary appears to match an individual or entity on a sanctions or restricted list. Restricted lists may include sanctions, terrorism financing, anti-corruption, politically exposed person, or other compliance-related lists. During the review period, transactions must not be cancelled, refunded, or otherwise released by an Agency until Viamericas Canada's Compliance Department has completed its review.

If a potential list match is identified, Viamericas Canada's Compliance Department will review the information to determine whether the match is confirmed. Until a determination is made, the transaction(s) will remain on hold.

Agents may not cancel transactions or return funds that are on hold due to list matches. Cancellation and return of funds may occur only after Viamericas Canada has authorized release.

If a match is confirmed, Viamericas Canada's Compliance Department will advise the Agency only of the operational disposition of the transaction (for example, whether it must be denied or cancelled). Any required regulatory, correspondent, or sanctions-related reporting will be completed by Viamericas Canada.

Listed Person or Entity Property Report

A Listed Person or Entity Property Report (LPEPR) is a mandatory report required under the Criminal Code of Canada when a transaction involves, or is attempted by or on behalf of, a person listed as a terrorist entity. LPEPR obligations exist in addition to reporting requirements under the PCMLTFA.

The List of Terrorist Entities is maintained by Public Safety Canada under section 83.05 of the Criminal Code. The list is available on the Public Safety Canada website (search for "Listed Terrorist Entities") and may be accessed at: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx.

If a sender or beneficiary appears to match a listed person, the transaction must not be released. If a match is confirmed, Viamericas Canada is required to hold (retain) the property involved in the transaction and report it in accordance with Criminal Code requirements. The term "property" includes funds associated with attempted or completed transactions.

Any required disclosures under the Criminal Code, including filing of LPEPRs with FINTRAC, will be completed by Viamericas Canada. Agencies must not submit LPEPRs directly and must not contact law enforcement, intelligence, or other authorities regarding potential matches.

Agencies will be advised only of the operational disposition of the transaction. Any required reporting, disclosure, or coordination with FINTRAC, law enforcement, intelligence, or other authorities will be completed by Viamericas Canada.

Ministerial Directives

Ministerial Directives are binding directives issued by the Minister of Finance under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) that impose specific measures on financial transactions involving certain jurisdictions. Ministerial Directives may require enhanced due diligence, additional reporting, or, in some cases, prohibit transactions.

Ministerial Directives apply in addition to standard AML/ATF requirements and take precedence where they impose stricter measures. Viamericas Canada's Compliance Department implements all applicable Ministerial Directives, including any related restrictions, enhanced reporting, or additional information requirements. Agencies are not required to monitor Ministerial Directives independently and should not attempt to interpret geopolitical or risk-related considerations.

As of the date of this guide, Ministerial Directives issued under the PCMLTFA apply to transactions associated with the following jurisdictions:

- Islamic Republic of Iran;
- Democratic People's Republic of Korea (DPRK); and,
- Russia

The full text of current Ministerial Directives is available on the FINTRAC website (search: "Ministerial

Directives") and may be accessed at: https://fintrac-canafe.canada.ca/obligations/directives-eng.

If a transaction involves a jurisdiction subject to a Ministerial Directive, Viamericas Canada's Compliance Department will determine whether the transaction may proceed and whether enhanced due diligence, additional reporting, or prohibition applies. Agencies will be advised only of the operational disposition of the transaction.

Additional Compliance and Customer Protection Measures

Fraud

In addition to AML/ATF obligations under the PCMLTFA, Agencies must remain aware of fraud risks that may affect their business or their customers. Fraud is distinct from money laundering and terrorism financing and may involve legitimate funds obtained through deceptive or unauthorized means. Fraud can result in financial loss, customer harm, reputational damage, and operational disruption.

Viamericas Canada expects Agencies to remain alert to fraud risks and to take reasonable steps to protect both the Agency and its customers from victimization.

Fraud is an extremely important and ever-increasing danger to you, your customers, and your business. Beyond the illegal measures attempted by criminals to engage in money laundering, etc., your agency can be at risk of victimization by several types of fraud at any time.

Impersonation Fraud

One common method of fraud involves impersonation of Viamericas Canada representatives. Criminals may attempt to obtain transaction information or request that Agencies configure or release transactions.

Viamericas Canada will never contact an Agency or customer to place test orders or to request sensitive transaction information, including transaction numbers or sender/beneficiary details.

If an individual identifies themselves as a Viamericas Canada representative and the call appears suspicious, contact Viamericas Canada immediately at 1-800-401-7626 or fraud_ops@viamericas.com.

Fraud Prevention Practices for Agencies

To help prevent fraud, Agencies should adhere to the following practices:

- Do not configure or send transactions based on instructions received by telephone.
- Do not discuss transaction details with anyone other than the customer (sender) or a verified Viamericas Canada representative.
- Do not send funds without first receiving payment from the customer.
- Ask reasonable questions to confirm the legitimacy of the transaction (e.g., “Do you know the beneficiary?”).
- Enter customer information accurately and completely.
- Do not allow P.O. Box addresses.
- Do not allow numbers or symbols in names.
- Provide accurate sender and beneficiary telephone numbers.
- Confirm destination cities to avoid misdirected payments.

- Remember that transactions on behalf of third parties or companies are not permitted.

Common Fraud Schemes Targeting Customers
Customers may be targeted by a variety of fraud schemes designed to persuade them to send funds to criminals. Common schemes include:

- Emergency or “Family in Trouble” Scams
  - A scammer claims that a friend or relative is in danger or needs immediate financial assistance.
- Romance Scams
  - Fraudsters develop false relationships online and request money from the victim.
- Prize or Lottery Scams
  - Victims are told they have won a prize and must pay fees to collect it.
- Job or Work Scams
  - Victims are persuaded to receive and re-send funds or to send money for “equipment” or “processing.”
- Advance Fee or Refund Scams
  - Victims are told they will receive money, but must send funds first.
- Consumer Purchase Scams
  - Customers send money for goods or services that are never delivered.

Responding to Suspected Fraud
If fraud is suspected at any point, do not proceed with the transaction. Contact Viamericas Canada’s Compliance Department or Fraud Operations Team for further guidance. Agencies may not contact suspected fraud perpetrators or attempt to verify the legitimacy of a scheme with third parties or beneficiaries.

Elder Abuse and Financial Exploitation

Older customers may be vulnerable to financial exploitation, including fraud and undue influence by third parties. Financial exploitation involves the unauthorized or deceptive use of an older adult's funds or property and may occur through coercion, persuasion, deception, or misuse of trust.

While Agencies are not required to investigate or determine whether financial exploitation has occurred, Viamericas Canada expects Agencies to remain alert to circumstances in which a customer appears confused, pressured, or directed by another person to complete a transaction.

If an Agency suspects that an older customer may be at risk of financial exploitation, the transaction should not proceed. The Agency should contact Viamericas Canada's Compliance Department for guidance.

Customers who believe they have been the target of a fraud scheme may contact the Canadian Anti-Fraud Centre for additional support at 1-888-495-8501 or visit https://antifraudcentre-centreantifraude.ca.

Protecting Customer Privacy

In the course of providing money services, Agencies collect personal information about customers, including identification information and other data required under the PCMLTFA. This information must be protected to prevent unauthorized access, misuse, identity theft, and fraud.

Customer personal information must be accessed only for legitimate business purposes, shared only with Viamericas Canada or other authorized parties for compliance or operational purposes, and stored securely in accordance with recordkeeping requirements.

Agencies must ensure that personal information retained for PCMLTFA recordkeeping purposes is protected against unauthorized access, loss, or disclosure. Personal information that is not subject to record retention requirements must be securely destroyed. Paper records should be shredded and electronic files should be deleted in a manner that prevents recovery.

Personal information may not be shared with customers, family members, or third parties unless required for compliance with applicable law or requested by Viamericas Canada. Privacy obligations do not prevent Viamericas Canada from sharing customer information with regulators, financial institutions, or law enforcement when required by law.

Banking and Safeguarding of Funds

Agencies collect funds on behalf of Viamericas Canada for the purpose of executing money transfers. Funds collected from customers are not Agency funds and must be deposited into the designated Viamericas Canada account assigned to the Agency. This account is used for the safeguarding and settlement of customer funds.

Deposits must reflect the full value of the prior day or days' transactions, including fees and commissions, and should be made in a single deposit. Funds collected for money transfer services may not be retained, commingled with Agency operating funds, or deposited into personal or business accounts other than the designated Viamericas Canada account.

The designated account is subject to the following requirements:

- The account must be used exclusively for deposits related to Viamericas Canada transactions.
- The account must not be shared with third parties or used for other business purposes.
- Deposits must not be separated, divided, or delayed for the purpose of altering deposit amounts or timing.
- Funds may not be deposited outside the province in which the Agency operates unless authorized by Viamericas Canada.

Failure to comply with banking and deposit requirements may result in the suspension of the Agency's standing with Viamericas Canada.

Non-Compliance and Consequences

Compliance with the PCMLTFA, the Criminal Code, the United Nations Act, and all related regulations is mandatory. Non-compliance may result in administrative, civil, or criminal consequences for both businesses and individuals. Potential consequences include:

- Administrative monetary penalties imposed by FINTRAC;
- Criminal prosecution for serious violations such as money laundering or terrorist financing;
- Loss of banking or correspondent relationships;
- Regulatory restrictions on the ability to conduct MSB activities; and,
- Suspension or termination of the Agency relationship with Viamericas Canada.

In addition, businesses may be held responsible for the acts or omissions of their employees in certain circumstances. Agencies are expected to maintain internal controls, ensure employees receive appropriate training, and follow Viamericas Canada's policies and procedures.

Viamericas Canada reserves the right to suspend or terminate Agency relationships where non-compliance is intentional, repeated, or negligent. While Viamericas Canada provides guidance, training, and tools to support compliance, each Agency and Agency employee remains responsible for complying with applicable laws, regulations, and Viamericas Canada policies.

Summary

Compliance with AML/ATF requirements is essential to the success of your Agency and to the protection of customers, financial institutions, and the broader financial system. At a high level, Agencies can support effective compliance by:

1. Maintaining an effective written AML/ATF program based on the Five Pillars;
2. Monitoring for, detecting, and escalating suspicious activity;
3. Collecting and retaining required customer information and records for five (5) years;
4. Completing periodic independent reviews of the compliance program;
5. Following Viamericas Canada's operational policies and procedures;
6. Safeguarding and depositing customer funds in accordance with designated banking procedures;
7. Protecting customer privacy and personal information;
8. Remaining alert to fraud and financial exploitation affecting customers; and,
9. Contacting Viamericas Canada with questions or concerns regarding compliance.

For questions, comments, or to report suspicious activity, please contact:

Viamericas Canada Compliance Department
1-877-382-0417
compliance@viamericas.ca