Agent and Agent Employee AML/ATF Compliance Training

Introduction

Introduction

This training is designed to assist all Viamericas Canada Agents and Agent Employees in:

- Creating a written **AML/ATF** Compliance Program;
- Designating a **Compliance Officer**;
- Complying with the **PCMLTFA** and its Regulations;
- **Safeguarding** customer funds and **non-public personal information**;
- Understanding **recordkeeping** and **reporting** requirements required;
- Conducting an **independent review**; and,
- Monitoring, detecting, and reporting **suspicious activity**.

Who Must Comply?

This training material, and the responsibilities set forth within, applies to the following parties:

- Agency Owners;
- Compliance Officers;
- Managers of your agency's business;
- Frontline Staff (for example, cashiers or tellers); and,
- Support Staff (any employees of the agency who may have access to customer information).

Terms Defined

Key Definitions

Understanding some key terms will help you identify and meet your compliance duties:

- **Agent**
  - A business authorized by Viamericas Canada to provide money transfer or other MSB activities on its behalf.
- **AML/ATF**
  - Short for “anti-money laundering/anti-terrorist financing”, this is the body of laws, policies, etc. designed to prevent the misuse of financial services for criminal activity.
- **Compliance Officer**
  - The person at the Agency responsible for the AML/ATF compliance regime.
- **FINTRAC**
  - This is Canada’s financial intelligence unit responsible for AML/ATF oversight of MSBs.
- **MSB (Money Services Business)**
  - A business engaged in money transfers, foreign exchange, or similar services. Viamericas Canada is a registered MSB, and Agents conduct MSB activities on its behalf.
- **PCMLTFA**
  - This is the primary AML/ATF law that sets the rules MSB and Agent compliance obligations.
- **Sender/Beneficiary**
  - The **Sender** is the customer initiating a transaction; the **Beneficiary** is the person designated to receive the funds.

Money Laundering and Terrorist Financing

What is Money Laundering?

Money laundering refers to:

- the handling or attempted concealment of funds related to illicit activity. Money transfers and other financial tools are commonly used in money laundering.

Money laundering happens in three stages:

- **Placement**: the introduction of illicit funds into a financial system;
- **Layering**: the movement of funds through multiple transactions or entities to obscure their origin; and,
- **Integration**: the re-entry of illicit funds into the economy as seemingly legitimate funds.

What is Terrorist Financing?

Terrorist financing refers to:

- the processing of funds to sponsor or facilitate terrorist activity.

A terrorist group seeks to create and maintain a system where whereby funds are sent to those who help terrorists. Funds used for terrorist financing may originate from both illegal and legitimate sources.

Structuring

Structuring is defined as:

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

For example, if a customer attempts to send two $500 transactions within the same day, they may be attempting to structure the larger amount in order to avoid a $1,000 reporting requirement.

It is illegal to structure transactions to avoid these requirements. It is also illegal for your agency to assist or aid a customer in structuring transactions.

It is your agency's responsibility to help prevent this form of money laundering.

Structuring

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.

Identifying Suspicious Activity

Identifying Suspicious Activity

To prevent money laundering, structuring, and other illicit activity, you must be able to detect and identify suspicious activity. **Suspicious activity** is:

- customer behavior, transaction patterns, or circumstances that appear unusual, inconsistent, or lacking a clear lawful purpose.

However, circumstances may vary from customer to customer and transaction to transaction. For example, one customer's money transfer transaction to Mexico may be normal, while another customer's similar transaction to the same location may be suspicious.

It is important to understand what is required to identify and prevent suspicious activity in your business.

Identifying Suspicious Activity

The following are some common examples of suspicious activity. A customer:

- asks how to avoid a reporting requirement;
- threatens or bribes you to not gather information;
- stops a transaction after you ask for information;
- requests a transaction that is unusually large compared to past transactions;
- provides a fake or altered ID;
- who regularly conducts transactions but does not appear to reside or work in the area where your agency is located;
- who sends to many different, unrelated beneficiaries; or
- or group of customers carry out high-value transactions at the same time.

Willful Blindness

Money laundering is a crime, and your agency has a responsibility to prevent it.

Active participation is:

- Aiding or allowing money laundering or terrorist financing to occur in your agency.

Willful blindness is:

- "looking the other way" or dismissing 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 difference** between active participation and willful blindness.

MSBs and Registration

MSBs and Registration

The **PCMLTFA** and related laws and regulations require that **MSB**s register with **FINTRAC**.

Viamericas Canada is an MSB and is required to register with FINTRAC. It must also maintain its list of Agents as part of this registration. Viamericas Canada Agents are required to provide complete and accurate information and to promptly notify Viamericas Canada of any changes to its business.

Note: If your business provides MSB services on its own, or as an agent of other MSBs, you may also be responsible for separate FINTRAC registration. Viamericas Canada does not maintain these registrations.

The PCMLTFA and Others

The PCMLTFA

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

Some measures established as a result of the PCMLTFA include:

- establishing record keeping and identification requirements for MSBs;
- requiring the reporting of suspicious financial transactions; and,
- establishing an agency (FINTRAC) that is responsible for dealing with reported information.

The PCMLTFA, and Others

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

- **Criminal Code**
  - The federal legislation that defines criminal offenses in Canada.
- **Ministerial Directives**
  - Binding directives issued by the Minister of Finance that can impose measures, restrictions, or prohibitions on transactions involving certain activities, countries, or persons.
- **Retail Payment Activities Act (RPAA)**
  - Administered by the Bank of Canada, this establishes federal oversight of retail payment service providers in Canada.
- **Revenu Québec**
  - The provincial authority administering licensing and oversight for MSBs operating in Québec.
- **Special Economic Measures Act**
  - Authorizes the Government of Canada to impose sanctions.
- **United Nations Act**
  - Enables the Government of Canada to implement decisions of the United Nations Security Council, including country-specific sanctions.

The Retail Payment Activities Act

The Retail Payment Activities Act

As mentioned, the **RPAA** is a federal law that regulates retail **payment service providers**, or PSPs. Viamericas Canada is considered a **PSP** under the RPAA; agents are <u>not</u>.

However, Agents must comply with all RPAA-related requirements established by Viamericas Canada. This includes:

- Safeguarding of Funds
  - Viamericas Canada and its Agents must protect end-user funds.
- Operational Risk Controls
  - Viamericas Canada and its Agents must maintain controls that reduce the likelihood of operational disruptions.
- Incident Reporting
  - Viamericas Canada, with assistance from its Agents, must report certain incidents, such as unauthorized access, system outages, errors or delays in release of end-user funds, etc. to the Bank of Canada.
- Recordkeeping
  - Agents of Viamericas Canada must maintain and provide upon request all records related to transactions, deposits, and more.

Compliance with RPAA

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 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);
- Establishing an Effective Written AML Program;
- Reporting;
- Recordkeeping;
- Periodic Independent Reviews; and,
- 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/ATF Program

The Five Pillars

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
- Pillar Two: Tailored Internal Policies, Procedures, and Controls
- Pillar Three: Ongoing Training
- Pillar Four: Independent Review
- Pillar Five: Risk and Customer Due Diligence

Pillar One: Designate a Compliance Officer

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 within the business, and may even be the Agency Owner, but it should be someone in a responsible position.

The Compliance Officer is responsible for:

(1) your Agency’s day-to-day compliance with AML/ATF policies, laws, and sanctions;

(2) for ensuring updates are received and enacted as required;

(3) for your Agency’s ongoing compliance training program;

(4) for adherence to Viamericas Canada’s RPAA Program; and,

(5) serving as the point of contact for escalation of suspicious activity.

Pillar Two: Tailored Internal Policies, Procedures, and Controls

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 items such as 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 submitted. 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 have reasonable grounds to suspect, that a transaction:

- involves founds derived from illegal activity;
- is designed to evade PCMLTFA requirements;
- services no business or apparent lawful purpose; or,
- involves use of an MSB to facilitate criminal activity.

Suspicious Transaction Report

Viamericas Canada will prepare and submit STRs **on your agency's behalf**, as well as in its own course of business.

However, it is important to understand the requirements of an STR narrative if Viamericas Canada requests further information.

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

A **Large Cash Transaction Report** (LCTR) must be filed with FINTRAC when $10,000 or more in cash is sent or received by the same person within 24 hours (single or multiple transactions). LCTRs must be filed within 15 days of the transaction.

Viamericas Canada's limits prevent customers from sending amounts that would trigger LCTRs. However, an LCTR may be required when an Agency makes cash deposits at a bank.

Information that may be required includes:

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

Large Cash Transaction Report

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**.

- These transactions are those that are conducted by someone who is not present at the time of the transaction. They are prohibited under the PCMLTFA and Viamericas Canada policy.

Viamericas Canada’s current transactional limits prevent customers from reaching this threshold.

Recordkeeping

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's "**Travel Rule.**"

- The Travel Rule requires that certain sender and beneficiary information accompanies money transfers (also EFTs) of $1,000 or more.

Recordkeeping

Your agency must record certain information for any transaction, regardless of the transaction type or method of payment. Our ViaOne system will request this information, and it includes:

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

Recordkeeping

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.

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

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.

Transactional Thresholds

These are the 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

Transactional Thresholds

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

- Full name;
- Full address;
- Telephone number(s);
- Full name of beneficiary;
- Full address of the beneficiary (if available);
- 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.

Transactional Thresholds

For transactions of **$1,000 to $2,999.99**, Viamericas Canada requires all of the prior information, plus:

- Government Identification Document type and number, and a copy of the ID document;
- Date of birth;
- Occupation;
- Street address of the beneficiary (required); and,
- The nature of the relationship between the sender and beneficiary.

Transactional Thresholds

For transactions of **$3,000 or above**, Viamericas Canada requires all of the prior information, plus:

- Name of the Customer's employer;
- Employer's phone number
- Purpose of transaction; and,
- Source of Customer's funds.

Transactional Thresholds

If you are required to collect a sender's identification, the following are acceptable forms of ID (provided that they are valid and current):

- Canadian Military ID;
- Canadian Driver License or ID Card
  - Issued federally or by a province or territory,
  - Quebec 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).

Transactional Thresholds

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.

If you believe information provided by a customer is false, Viamericas Canada recommends that you not complete the transaction.

Submitting ID Copies

In order to approve transactions, Viamericas Compliance must receive a copy of any identification documents presented. These documents may be submitted to the Viamericas Canada 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.
- **ViaMobi**: Take a photo using a mobile phone and send it directly to our Compliance Department: https://www.viamericas.mobi
- **QR Code**: Locate the QR code in the customer's ViaOne profile.
- **E-mail**: Scan the document and send it to ID@viamericas.com
- **Fax**: Send documents to 1-800-490-8147. Make sure to include the following information on 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. The KYC Form is required when a customer's transactions exceed thresholds 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.

Know Your Customer

The **KYC 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 each review and sign the completed form.


VIAMERICAS

Know Your Customer Form
Last revised 10/1/2021

KNOW YOUR CUSTOMER (KYC) FORM
(FORM A 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 (Ocupación): ____________

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. También 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 certain transactional thresholds. These "**aggregation**" reviews may require additional information, including identity verification or completion of a "short" or "long" KYC Form.

During an aggregation review, transactions must not be cancelled, refunded, or released until Compliance completes its review. Agents may not bypass an aggregation hold by cancelling and reinitiating transactions.

If additional identity information is required, ViaOne will notify. Transactions remain on hold until information is submitted or Viamericas Canada cancels them.

Pillar Three: Ongoing Training

Ongoing Training

Your Agency should establish an **ongoing training** program for Owners, Compliance Officers, and all Employees who have any involvement in the business's MSB activities. This program should be managed by the **Compliance Officer**.

Training should be thorough and complete and must include all relevant information prior to any employee conducting MSB-related transactions. It should be completed upon onboarding and at least annually. Completion of training must be documented and retained.

Viamericas Canada provides the ViaAcademy training platform. This, as well as the ViaOne Resource Center, can be accessed through ViaOne.

Pillar Four: Independent Review

Independent Review

Your Agency must complete an **independent review** of its AML/ATF and RPAA compliance regime. Viamericas Canada requires Agencies to conduct independent reviews at least once per year.

The independent review may be performed by a responsible employee of your Agency who does not report to the Compliance Officer. The review also **may not be conducted** by your Agency's Compliance Officer. However, the Compliance Officer is responsible for ensuring that the independent review is completed.

An independent review checklist can be found within the ViaOne Resource Center.

Pillar Five: Risk and Customer Due Diligence

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.

These are focused more intently on establishing positive identity of your customer, especially those that represent a potentially higher risk.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) is a KYC process that provides extra scrutiny of certain customers and their transactions. It highlights risks that may not be identified through standard due diligence.

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

PEPs, HIOs, and RCAs

Viamericas Canada does not permit certain customers to transact due to elevated corruption and financial crime risk. Customers identified as belonging to any of these categories cannot send or receive transactions through Viamericas Canada.

Politically-Exposed Persons

- A PEP is an individual who is or has been entrusted with prominent public functions by a country, province or state, or local municipality.

Heads of International Organizations

- These 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 include senior United Nations members, and the President of the World Bank.

Relatives and Close Associates

- These 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.

List Match Reporting

Transactions may be placed on **hold** when a sender or beneficiary appears to match an individual or entity on a restricted list (such as sanctions, terrorism financing, PEP, or other compliance-related lists).

During this review period, **Agents must not cancel, refund, or release funds** until Viamericas Canada's Compliance Department completes its review and authorizes next steps. You will be able to view the status of the transaction in ViaOne.

Viamericas Canada's Compliance Department will determine if the match is confirmed. Only after Compliance authorizes release may the transaction be cancelled, or funds returned to the sender.

Listed Person or Entity Property Report

A **Listed Person or Entity Property Report** (LPEPR) is a mandatory report 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.

If a sender or beneficiary appears to match a listed person, the transaction must not be released and funds cannot be returned. If a match is confirmed, Viamericas Canada is required to hold the funds and file the report.

Viamericas Canada will complete any required LPEPRs. Agencies must not submit LPEPRs directly.

Ministerial Directives

Ministerial Directives are issued by the Minister of Finance that impose specific measures on financial transactions involving certain jurisdictions. They may require enhanced due diligence, additional reporting, or, in some cases, prohibit transactions.

Ministerial Directives take precedence over AML/ATF obligations where they impose stricter measures. Viamericas Canada's Compliance Department implements all applicable directives.

Ministerial Directives currently issued apply to transactions associated with the following jurisdictions:

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

Additional Compliance and Customer Protection Measures

Fraud

Agencies must remain aware of fraud risks that may affect their business or their customers. **Fraud** is distinct from ML/TF 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.

Beyond the illegal measures attempted by criminals to engage in illicit activity, 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

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 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 (For example, “Do you know the beneficiary?”).
- Enter customer information accurately and completely.
- Do not allow P.O. Box addresses, or numbers or symbols in names.
- Be sure to 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
- Romance Scams
- Prize or Lottery Scams
- Job or Work Scams
- Advance Fee or Refund Scams
- Consumer Purchase Scams

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

viaAcademy

Older customers may be even more vulnerable. **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.

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, the transaction should not proceed, and Viamericas Canada should be contacted.

Canadian Anti-Fraud Centre: 1-888-495-8501 or https://antifraudcentre-centreantifraude.ca.

Protecting Customer Privacy

Agencies collect customer **non-public personal information** (NPPI), including identification data, and must protect it against unauthorized access, misuse, identity theft, and fraud. Customer information may be accessed only for legitimate purposes, shared only with Viamericas Canada, and stored securely.

Information retained must be protected, and information not retained must be destroyed. NPPI may not be shared with customers, family, or third parties unless required by law or requested by Viamericas Canada.

In Canada, NPPI privacy obligations are governed by **PIPEDA**, which is:

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

Banking and Safeguarding of Funds

Banking and Safeguarding of Funds

- Agencies collect funds on behalf of Viamericas Canada to execute money transfers. These funds are **not Agency funds** and must be deposited into the designated Viamericas Canada account assigned to the Agency for safeguarding and settlement.
- Deposits must reflect the full value of prior day(s) transactions (including fees and commissions) in a **single deposit**. Funds may not be retained, commingled with Agency operating funds, or deposited into personal or business accounts.
- Designated Account Requirements**:**
  - Used exclusively for Viamericas Canada deposits;
  - Not shared with third parties or used for other business purposes;
  - Deposits may not be separated, divided, or delayed; and,
  - Funds may not be deposited outside the province of operation without authorization.

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

Non-Compliance and Consequences

Non-Compliance and Consequences

Compliance with all involved laws and regulations, as well as Viamericas Canada's policies, is mandatory. **Non-compliance** may lead to:

- Administrative monetary penalties imposed by FINTRAC;
- Criminal prosecution for serious violations;
- Loss of banking relationships;
- Regulatory restrictions on MSB activities; and,
- Suspension or termination of the Agency relationship.

Agencies must maintain controls, ensure training, and follow Viamericas Canada policies and procedures.

Viamericas Canada may suspend or terminate Agency relationships where non-compliance is intentional, repeated, or negligent. While support and guidance are provided, **each Agency and employee remains responsible for compliance** with applicable laws and policies.

Summary

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. Agencies can support effective compliance by:

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

Thank you!

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

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