



ANTI-MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION COMPLIANCE PROGRAM

TABLE OF CONTENTS

SECTION 1 – USER INFORMATION

SECTION 2 – ANTI-MONEY LAUNDERING COMPLIANCE OVERVIEW

SECTION 3 – COMPLIANCE OFFICER

SECTION 4 – EMPLOYEE TRAINING

SECTION 5 – SUSPICIOUS ACTIVITY

SECTION 6 – RECORD KEEPING AND REPORTING REQUIREMENTS

SECTION 7 – KNOW YOUR CUSTOMER

SECTION 8 – RESPONSE TO LAW ENFORCEMENT REQUESTS

SECTION 9 – INDEPENDENT REVIEW OF AML COMPLIANCE PROGRAM

AMENDMENT A – ANTI-MONEY LAUNDERING COMPLIANCE EMPLOYEE TRAINING GUIDE

AMENDMENT B- SUSPICIOUS ACTIVITY/TRANSACTION REPORT

SECTION 1 USER INFORMATION

INSTRUCTIONS

This document contains policies and procedures to help your business comply with Anti-Money Laundering Regulations. In order for this document to be considered an adequate AML program, you must:

Document business specific policies and procedures including, but not limited to designation of the Compliance Officer, Money Services Business Registration, scheduling employee training, acceptable IDs, transaction limits, and / or easy to follow instructions for employees to follow.

Review and update this document on a periodic basis to ensure that the contents and procedures are current and reflect actual business practices.

LEGAL DISCLAIMER

Although this document contains legal information, it is not intended to be, nor should it be considered legal advice.

For legal advice, including the interpretation and application of any law, please consult our attorney.

CIVIL & CRIMINAL SANCTIONS

The penalties for violating regulations are severe, and under certain circumstances, may be assessed against a business and / or one or more employee(s).

Violations may cause loss of customer goodwill and unfavorable publicity, as well as civil and criminal penalties.

All persons who sell, offer and / or process money orders, cash cheques, pay day loans must be aware that liability may be imposed on them if the business and / or employee is willfully blind to suspicious activity or knew information that he / she "should have known" was suspicious.

Any employee that violates these policies and procedures, either unknowingly or intentionally may be subject to disciplinary action, including but not limited to, civil penalties, criminal penalties and termination of employment.

SECTION 2

ANTI-MONEY LAUNDERING COMPLIANCE OVERVIEW ADOPTION OF ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

Store Number and Manager

to be known herein as the 'Business'
hereby certifies and adopts the policies and procedures contained in this document,
as its Anti-Money Laundering (AML) Compliance Program.

Print Name Title

Signature Date

STATEMENT OF POLICY

The Business supports the fight against money laundering and terrorism; it has adopted this AML Compliance Program to prevent its financial services from being used to promote criminal activity.

The Business will fully comply with both the intent and letter of all laws and regulations relating to AML, the prevention of terrorist financing and economic sanctions. The manager will train its employees to comply with these laws and regulations.

A copy of this AML Compliance Program will be kept at each location conducting money services business (MSB), in a place that is accessible to employees conducting MSB transactions. Every employee who conducts or is involved in Money Services Business operations is required to understand and comply with the contents of this document.

MONEY LAUNDERING DEFINITION AND DESCRIPTION

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. If illegal money is successfully laundered, criminals maintain control over their illegally obtained funds and they can establish a separate cover for their illicit source of income. The AML laws apply to any funds derived from illegal activities, such as funds held by drug traffickers, terrorists, organized crime, tax evaders and other groups and individuals seeking to transfer, spend and / or invest money derived from any type of crime.

The money laundering cycle includes placing funds into the financial system by initiating Pay day loans cheque cashing or buying money orders or sending/receiving money orders. Once the funds have entered the system, the source of illegal funds is further disguised by transferring them through layers of financial institutions, such as bank or investment accounts. Finally, the funds are legitimized by purchasing items or investing in legitimate investments such as real estate, real property, stocks and bonds.

Money laundering is not limited to cash; money laundering can be done through any type of financial transaction, including, but not limited to, funds transfers, cheque cashing, cheques, debit cards, stored value and credit card transactions.

TRANSACTION MONITORING

The Compliance Officer will establish procedures for the review of higher-risk, out-of the-ordinary transactions involving money transfers and money orders in order to identify transactions that may require special record keeping or reporting, including the reporting of suspicious activity.

MONEY SERVICES BUSINESS (MSB)

As a provider of financial services and products our Business is a money services business (MSB). MSBs are defined as any business that provides or sells:

- Money transfer services in any amount
- Money orders, travelers cheques or stored value items of \$1,000 or greater to any person in one or more transaction in one day
- Cheque cashing services and / or currency exchanges of \$1,000 or greater for any person in one or more transaction in one day
- Pay day loan services

SECTION 3

THE COMPLIANCE OFFICER

Name of Person	Compliance Officer Title
----------------	-----------------------------

is hereby designated as the Anti-Money Laundering Compliance Officer. **COMPLIANCE OFFICER RESPONSIBILITIES**

The Compliance Officer as well as a senior manager's responsibilities includes: Ensuring ongoing compliance with all government AML regulations.

- Coordinating the AML Compliance Program.
- Reviewing and updating the AML Compliance Program as necessary due to changes in laws or regulations and ensuring that all affected employees have been advised of these changes.
- Ensuring that all employees are trained on AML compliance requirements before conducting MSB transactions.
- Ensuring regular AML training is conducted in an effective manner for all appropriate employees.
- Ensuring all training is documented, including the date of the training, name of the trainer/trainee and topics discussed.
- Monitoring day-to-day compliance with the related laws and regulations.
- Ensuring accurate record keeping and reporting as mandated by the home office. Ensuring that the AML Compliance Program is subjected to periodic independent reviews.
- Cooperating with law enforcement and AML investigations.

SECTION 4

EMPLOYEE TRAINING

TRAINING REQUIREMENTS

Training must be provided to all employees who are involved with MSB transactions and at a minimum must include:

1. Identifying suspicious activity and structured transactions,
2. Record keeping and reporting requirements,
3. Verifying customer identification, and
4. Familiarity with AML forms.

Before conducting any MSB transactions, new employees are required to understand and comply with the contents of this AML Compliance Program and sign an acknowledgement form that will be retained in their personnel file or with the AML files.

Existing employees who conduct MSB transactions will receive periodic refresher AML training that will be documented and retained in their personnel file or with the AML files.

Amendment A of this AML Compliance Program provides an overview of this AML Compliance Program that can be used to help train employees.

SCHEDULING EMPLOYEE TRAINING

The Business Compliance Officer will schedule and ensure periodic employee AML training is conducted:

- Every month
- Semi-Annually (every 6 months)
- Annually (every 12 months)
- Every 18 months
- Bi-Annually (every 24 months)
- As necessary
- Other:

SUSPICIOUS ACTIVITY

SUSPICIOUS ACTIVITY REPORT BY MONEY SERVICES BUSINESS (SAR-MSB)

The federal government requires that Money Service Businesses file Suspicious Activity Report by Money Services Business (SAR-MSB) for any transaction – or pattern of transactions – that is attempted or conducted with at least \$2,000, if an employee knows, suspects or has reason to suspect that the activity:

1. Involves funds derived from illegal activity or is intended to hide funds derived from
Illegal activity
2. Is structured to avoid record keeping or reporting requirements
3. Has no business or apparent lawful purpose
4. Facilitates criminal activity

Transactions totaling less than \$2,000 can be reported at the Business' discretion.

The Compliance Officer shall report suspicious transactions by filing a SAR-MSB within 30 calendar days of the detection of the suspicious event.

In situations involving violations that require immediate attention, such as ongoing money laundering schemes or potential terrorist financing, immediate notice by telephone shall be given to appropriate law enforcement authorities in addition to filing the SAR-MSB. The SAR-MSB must be completed in accordance with the instructions provided with the SAR-MSB form.

Employees must not alert the customer conducting the suspicious transaction of their suspicions or that a SAR-MSB has been or will be filed.

A suspicious activity file, including blank copies of SAR-MSBs, must be kept in a secure location at each store and will be accessible at all times.

STRUCTURING

Structuring is the act of breaking up large transactions into several smaller transactions to avoid providing personally identifying information.

Many money launderers are familiar with the dollar thresholds that require record keeping and reporting; to remain anonymous and avoid the detection of law enforcement officials, money launderers attempt to process transactions to avoid triggering record keeping and / or reporting requirements. The processing of transactions that avoid record keeping and / or report requirements is known as structuring.

Money launderers may also attempt to trick employees into allowing them to structure transactions by splitting up transactions with several accomplices or by trying to "con" employees with a hard luck story. Employees need to be on the lookout for structuring so that they can prevent it from occurring.

It is illegal to structure transactions or to help customers avoid record keeping or reporting requirements. Employees may not tell or even imply to a customer that he / she can avoid providing information by conducting smaller transactions.

The following examples of potential structuring are specifically designed to avoid record keeping requirements that should be reported for further research, review and possible SAR-MSB filing.

1. A customer asks to purchase six (6) money orders or money transfers for \$500 each, totaling \$3,000.
2. Early in the morning, a customer purchases four (4) money orders or money transfers for \$500 each, totaling \$2,000. Later in the day, the customer returns and purchases an additional four (4) money orders or money transfers for \$500 each. When combined, the eight transactions total \$4,000.
3. A customer asks to send four (4) money transfers for \$850 each totaling \$3,400 on the same day to the same receiver.

It is illegal for the Business, its employees or customers to structure transactions in order to avoid the record keeping or reporting requirements.

Employees should never help anyone structure a transaction to avoid AML reporting or record keeping requirements.

Employees should never tell customers how to avoid any transaction limitation.

SUSPICIOUS ACTIVITY/TRANSACTION REPORT

Suspicious activity can vary from one transaction to another based on the circumstances surrounding the transaction or group of transactions. One customer's transaction(s) may be normal based on your knowledge of that customer, while another customer's transaction(s) may be suspicious.

Many factors are involved in determining whether transactions are suspicious, including, but not limited to the amount, the location of the store, comments made by the customer, the customer's behavior and the customer's previous transaction history.

The following list provides examples of potentially suspicious activity that should be reported for further research, review and possible SAR-MSB filing.

- A customer or employee appears to structure transactions in an attempt to avoid AML record keeping or reporting requirements.
- An individual provides minimal or fictitious information concerning their name and other identifying data.
- A customer engages in a discussion with an employee to try to determine ways to avoid reporting or record keeping requirements.
- A customer buys one or more money orders several times a day, or over several days that when added together exceed the \$3,000 record keeping limit.
- A customer uses a false or obviously altered ID.
- A customer is unable or unwilling to provide ID.
- Two or more customers use the same or similar IDs.
- A customer tries to alter his / her transaction after being asked to show ID.
- A customer deliberately changes the spelling of his / her name on multiple transactions.
- A customer states he / she does not have a local address but he / she appears to reside locally because he / she is a repeat customer.
- Two or more customers apparently work together to break one transaction into two or more transactions to avoid record keeping requirements.

- A customer uses two or more locations or cashiers in the same city on the same day to process transactions or purchase money orders.
- A customer offers bribes, tips or threatens employees to avoid record keeping requirements.
- A customer admits that the cash for his / her transactions came from illegal conduct.
- A customer makes large transactions that are not consistent with his / her occupation or business practice.

REPORTING STRUCTURING AND SUSPICIOUS ACTIVITY/TRANSACTION REPORT

1. Employees will report all suspicious activity to the Compliance Officer or an assigned delegate, regardless of the dollar amount.
2. The Compliance Officer or an assigned delegate will investigate the activity to determine if the activity is suspicious.

If the activity is suspicious, The Compliance officer will within 30 days of detection of the suspicious activity complete SAR_MSB forms which will be mailed to Mr. Cory McGinness at the head Office of Moneymate.

A copy of the filed SAR-MSB must be maintained in the Suspicious Activity file for five (5) years.

If the activity is not suspicious, the Compliance Officer will document the reason and will keep the documentation for a minimum of five (5) years in the AML files.

3. Copies of filed SAR-MSB forms and any supporting documentation must be maintained in the AML files for five (5) years and made available to appropriate law enforcement and regulatory agencies upon request. Supporting documentation must be identified in the Narrative Section of the SAR-MSB.

SECTION 6

RECORD KEEPING AND REPORTING REQUIREMENTS

All reporting and record keeping procedures are designed to comply with Regulations. Complying with the AML Regulations requires the Business to:

1. Keep records of cash purchases of monetary instruments (e.g., money orders, cheque cashing) of \$3,000 to \$10,000.
2. Keep records of money transfers of at least \$3,000 or too frequent card loads.
3. File suspicious activity reports (SAR-MSBs).
4. Obtain and retain other records as necessary.

COLLECTION OF CUSTOMERS' INFORMATION

When processing MSB transactions for customers, the customer may be asked to prove his / her name and address in addition to other information as required by the Federal and Provincial AML Regulations, including, but not limited to:

- Physical Address
- Government issued ID
- Social Insurance Number or Tax identification

- Date of Birth
- Occupation
- Any other company mandated information

The customer must provide a physical address where he / she resides. A post office box (P.O. Box) is not acceptable unless the P.O. Box is listed as the customer's official address on his / her photo ID. The customer CANNOT use the Businesses address to process a transaction.

When documenting a customer's photo ID, the Business will include the type of ID, the ID number, and the issuer of the ID.

A SIN or TIN is unnecessary if the customer lives and works outside of Canada and presents a passport issued by a foreign government.

If a customer refuses to provide the information required by Federal and / or Provincial AML Regulations, the Business CANNOT process the transaction.

THIRD PARTY INFORMATION

If the customer who is conducting a transaction (that is eligible for 3rd party initiation) is doing so for someone else, the information must be obtained for both parties. Examples of third parties are an employee of a business conducting the transaction for the business, or a relative of an elderly or disabled person conducting the transaction for that person. Complete the Multiple Persons or Third Party sections on reporting and record keeping forms.

MAINTENANCE OF RECORDS

All record keeping and reporting documentation will be maintained for a minimum of five (5) years and they will be made readily available to the authorities upon request.

In accordance with the Privacy Act, the Business will protect customers' personal and private information. All documents that contain customers' private and personal information will be stored in a secure location. If the Business discards any MSB documents, the documents must be completely destroyed prior to disposal.

PROVINCIAL SPECIFIC REQUIREMENTS

The reporting/record keeping requirements and monetary thresholds may vary by province. The Business will follow the provincial laws where they are stricter than the Business' own policies, otherwise the Business' policies will prevail.

ACCEPTABLE FORMS OF PHOTO IDENTIFICATION

When processing MSB transactions for customers, the customer may be required to provide a valid form of government issued photo ID to verify the customer's identity. The customer's name and picture must match the information and picture on the photo ID.

If the customer indicates that he / she is not a resident of Canada he / she must present a passport, alien identification card or other official document evidencing nationality or residence.

Photo identification presented to process an MSB transaction must be issued by a legitimate government agency and must include a picture and expiration date.

The Business must deny any presented form of identification that is expired or appears to be altered or fabricated.

CASH PURCHASES OF MONEY ORDERS OR DEBIT CARDS

Whenever a customer uses cash to purchase money orders for amounts between \$3,000 and \$10,000, specific information about the purchaser must be collected; purchases of money orders for more than \$10,000 in cash require supervisor authority and reporting.

Money order purchases or card fills made in one business day must be aggregated, or added together, and treated as a single purchase. Multiple purchases made in one day totaling \$3,000 or more must be documented on the daily report.

The Daily report should be accessible to all employees who cash cheques sell money orders, initiate pay day loans. Completed Daily reports must be maintained in the store for five (5) years.

PROCESSING CASH PURCHASES OF MONEY ORDERS OR DEBIT CARDS

1. Each employee will log single and / or multiple money order purchases of \$3,000 or more, that are purchased on or behalf of one customer in one day.
2. For any money order transaction of \$3,000 or more (single or aggregate per day) the employee must obtain and record, on a Log, the following information about the purchaser **BEFORE** completing the transaction:
 - Name
 - Address
 - Valid government issued photo ID
 - Social insurance number or tax identification number, if purchaser is Canadian resident
 - Date of birth
 - Third party info and Trans/date
 - Serial number of money order(s)
 - Amount of each money order purchased Total amount purchased
3. The Business retains the right to refuse to process any transaction that appears suspicious.

REQUIRED CUSTOMER INFORMATION ON MONEY TRANSFER RECEIVE TRANSACTIONS

Specific customer information must be documented at different receive transaction amounts. At all transaction receive amounts, the customer receiving a money transfer must provide appropriate information and / or documentation to the Businesses satisfaction to demonstrate the right to receive the transaction.

The receive customer's information must be documented **BEFORE** the transaction is processed:

\$0.00 - \$2999.99

Name
Address
Transaction amount
Transaction date
Valid government issued photo ID

If the receive customer does not have acceptable Photo ID, test questions are permitted to receive money transfers up to \$899.99.

\$3,000.00 - \$10,000.00

Name
Address
Transaction amount
Transaction date
Valid government issued photo ID
Social insurance number or tax identification number, if receiver is US citizen / resident.
Date of birth
Specific occupation

The customer's information should be documented on both the front and back of the store copy the customer must sign the store copy Record keeping requirements:

*all transactions under \$3,000 be maintained for at least 6 months.
Transactions of \$3,000 or more must be retained for five (5) years in the
Businesses AML files.*

BUSINESS TRANSACTION LIMITS FOR MONEY TRANSFER RECEIVE TRANSACTIONS

The Manager processes receive transactions.

The Manager's limit for an individual money transfer receive transactions for one person in a single business day at the maximum amount of:\$3000 The Manager limits combined money transfer receive transactions for one person in a single business day for at maximum amount of \$3000

*Transactions that are structured at or below AML Compliance thresholds should be considered Suspicious Activity and should be filed on a SAR-MSB.
The manager is solely responsible for ensuring money transfer receive limitations are enforced.*

PROCESSING RECEIVE TRANSACTIONS

1. Prior to conducting any transfer transaction, the Manager will verify the customer completes all appropriate and necessary sections and signs all forms. If the Manager does not use all appropriate forms for whatever reason the Manager will ensure the customer signs the receipt.
2. The employee processing the transaction will correctly input the information provided by the customer into transfer system.

3. The Business may require a customer to provide personally identifying information **BEFORE** completing any MSB transaction depending on the type, amount or circumstances surrounding the transaction.
4. The Business retains the right to refuse to process any transaction that appears suspicious.

KNOW YOUR CUSTOMER

One of the most effective ways to protect a business from becoming the victim of financial crimes starts with verifying the identity of the customers and knowing with whom MSB transactions are conducted.

To avoid processing transactions that could put the Business at risk, the Business will implement a ‘Know Your Customer’ policy that includes, but is not limited to:

- Only accepting valid, government issued photo ID documents, such as a driver’s license, passport or alien identification card that contains the customer’s name, address and photograph.
- Requesting and documenting required customer information before processing transactions
- Monitoring customer transaction activity

RESPONSE TO LAW ENFORCEMENT REQUESTS AUTHORITY TO SUMMON TESTIMONY AND RECORDS

Government regulators and law enforcement agencies may seek information and records from time to time. Any person associated or connected with the Business who receives or is served with a summons, subpoena or court order related to any transaction the Manager should immediately contact the head office of Moneymate for assistance.

The Business will assist these entities in their investigations, provided the request(s) is / are conducted in a lawful manner. This is necessary to ensure that the Business complies with customer privacy laws. Furthermore, government agents are not permitted to use their summons authority to go on unwarranted “fishing” expeditions in our records. Employees should not feel pressured by government agents to release consumer or company information without first receiving a proper summons, subpoena or court order.

Any person subpoenaed or asked to disclose a SAR-MSB or the information contained in it, except where the request is by an appropriate law enforcement or supervisory agency, must not produce the SAR-MSB or provide any information that would disclose that a SAR-MSB has been prepared or filed.

SECTION 9

INDEPENDENT REVIEW OF AML COMPLIANCE PROGRAM

The Business will conduct periodic independent reviews of its AML Compliance Program as required by Federal AML Regulations. The Independent Review will be conducted by a person or persons who are knowledgeable about the AML requirements that apply to MSBs.

The Business' Independent Review cannot be conducted by the Business' designated Compliance Officer. or any company representative.

The Business will conduct / conducted an Independent Review of its AML Compliance Program on:
Month Day Year

The Independent Review of the Businesses AML Compliance Program was conducted

by:

The Business Compliance Officer will schedule and ensure an Independent Review of the Businesses AML Compliance Program:

1. Semi-Annually (every 6 months)
2. Annually (every 12 months)
3. Every 18 months
4. Bi-Annually (every 24 months)
5. As necessary
6. Other:

AMENDMENT A

ANTI-MONEY LAUNDERING COMPLIANCE EMPLOYEE TRAINING

Businesses and their employees who conduct MSB transactions must understand:

The concept of money laundering
How to identify suspicious activity

How to comply with the record keeping and reporting requirements

STRUCTURING AND SUSPICIOUS ACTIVITY

Structuring is the act of breaking up potentially larger transactions into several smaller ones in order to avoid record keeping or reporting requirements.

Suspicious Activity is based on many different factors, including the amount of the transaction, the location of the business, comments made by the customer, the customer's behavior, etc. Suspicious activity may be very different from one transaction to another based on all of the circumstances involved.

SUSPICIOUS ACTIVITY REPORT BY MONEY SERVICES BUSINESS (SAR-MSB)

A **SAR-MSB** must be filed for any transaction, or pattern of transactions, that is attempted or conducted that is at least \$2,000, where it is known or suspected that the transaction:

Involves funds derived from illegal activity or is intended to hide funds derived from illegal activity

Is structured to avoid record keeping or reporting requirements Has no business or apparent lawful purpose, or

Facilitates criminal activity

If suspicious activity occurs, the business must:

File SAR-MSBs according to the instructions on the form and include as much information as is known about the customer

Record these transactions on a Log, if necessary (filing a SAR-MSB does not satisfy any other record keeping requirements).

Retain the SAR-MSBs for five (5) years

RECORD KEEPING FOR MONEY ORDER PURCHASES FROM \$3,000 to \$10,000

Record transactions on a must contain:

Customer's name Customer's address

Customer's valid, government issued photo ID

Customer's date of birth

Customer's social insurance number

Store address

Date of purchase

Money order serial numbers

Money order amounts

Total transaction purchase amount

The daily reports must be retained by the Business for five (5) years.

RECORD KEEPING FOR MONEY TRANSFER SEND TRANSACTIONS

Customer name

Customer address Transaction amount

Transaction date

\$900.00 - \$2999.99

Customer name

Customer address

Transaction amount

Transaction date

Customer's valid government issued photo ID

\$3,000.00 - \$10,000.00

Customer name
Customer address
Transaction amount
Transaction date
Customer's valid government issued photo ID

Customer's social insurance number or tax identification number (unless the customer lives and works outside Canada and presents a Passport or ID issued by a foreign government)

Customer's date of birth
Customer's specific occupation

Single or multiple transactions, totaling \$9,100. or greater require that other service providers AML must be observed

RECORD KEEPING FOR MONEY TRANSFER RECEIVE TRANSACTIONS

In addition to identifying the receive customer's right to receive the transaction, the following receive customer's information must be documented **BEFORE** the transaction is processed:

\$0.00 - \$2999.99

Name
Address
Transaction amount
Transaction date
Valid government issued photo ID

If the receive customer does not have acceptable photo ID, test questions are permitted to receive money transfers up to \$899.99.

\$3,000.00 - \$10,000.00

Name
Address
Transaction amount
Transaction date
Valid government issued photo ID
Social insurance number or tax identification number, if receiver is Canadian resident
Date of birth
Specific occupation