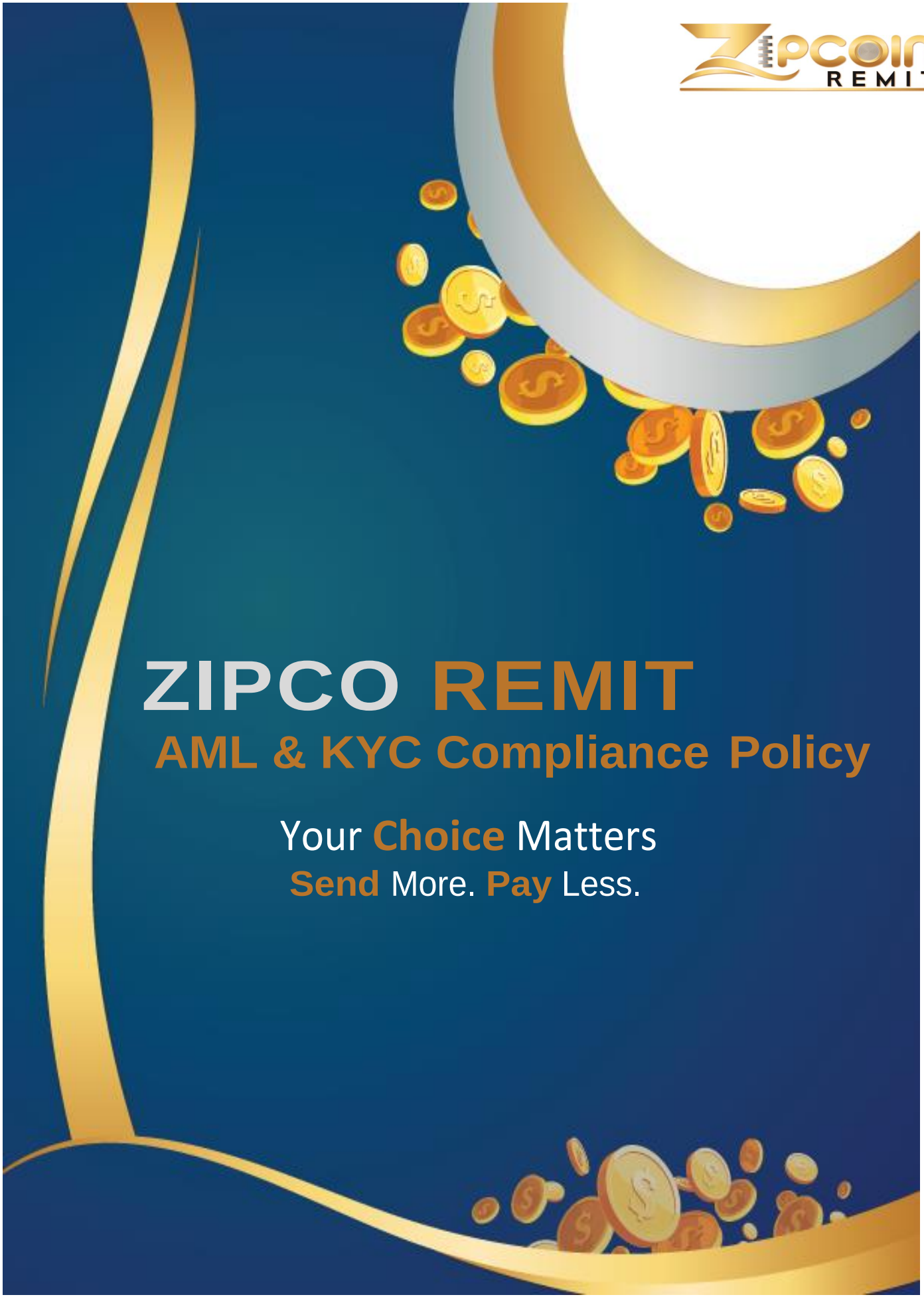

ZIPCO REMIT

AML & KYC Compliance Policy

Your **Choice** Matters

Send More. **Pay** Less.

Table of Contents

AML & KYC Compliance Policy

Last Updated: 15 April 2019

1. AML & KYC Compliance Policy

ZipCoin Remit Canada Ltd. referred to throughout this policy as “ZIPCO Remit” or ZipCoin or “ZIPCO”- has developed an Anti-Money Laundering and Anti-Terrorist Financing Policy that meets legislative requirements and reflects management’s principles on managing money laundering and terrorist financing risks posed to ZIPCO Remit.

ZIPCO Remit is registered with the Financial Transactions and Reports Analysis Centre of Canada (“FINTRAC”) as a Money Service Business (“MSB”) and cooperates fully with FINTRAC and other law enforcement agency requests in their efforts to detect, prevent, and deter money laundering and terrorist financing.

It is the responsibility of our Board of Directors and Senior Management to ensure that ZIPCO Remit maintains this effective internal control structure, including suspicious activity monitoring and reporting. ZIPCO Remit’s AML Program is based upon the:

1. Nature, scale and complexity of ZIPCO Remit’s business;
2. Diversity of ZIPCO Remit’s operations, including geographical diversity;
3. ZIPCO Remit’s customer, product and activity profile;
4. Distribution channels used;
5. Volume and size of the transactions;
6. Degree of risk associated with each area of ZIPCO Remit’s operation; and
7. The extent to which ZIPCO Remit is dealing directly with the customer or is dealing through intermediaries, third parties, correspondents, or non-face to face access.

Changes to this policy require approval by the Board of Directors, Partners, owners (known hereafter as “Managers”) of the ZIPCO Remit.

Changes in operating procedures, standards, guidelines and technologies, provided they are consistent with this policy, may be authorized by the ZIPCO Remit.

The “Managers” have the authority to approve this policy, and annually approves the merit thereafter. Management is responsible for ensuring the directives are implemented and administered in compliance with the approved policy.
The primary responsibility for enforcement of this policy and its operating procedures rests with the “Managers” and our employees.

2. Definitions

- **Money Laundering** - An activity criminalized by law.
- **Terrorist**- an act of domestic terrorism or international terrorism.
- **Accoun**t- a formal business relationship established to provide regular services, dealings and other financial transactions, and includes, but is not limited to, trading, remitting funds, etc
- **Transaction** - a credit or group of credits and their associated debits.
- **CAMLO**- Chief Anti Money Laundering Officer

3. Structure of Accountability

1. "Managers" have the ultimate responsibility to ensure the proper management of ZIPCO Remit's AML Program. To this end, the "Managers" have the responsibility to determine the necessary course of action to ensure adherence to appropriate laws and regulations are managed in an effective and consistent manner for the entire organization.

   Specifically, the "Managers" are responsible for:

   A. Ensuring the quality of ZIPCO Remit's AML Program
   B. Designating a qualified CAMLO;
   C. Maintaining a working knowledge of ZIPCO Remit's AML Program; and
   D. Reviewing for formal adoption the written policies and procedural guidelines necessary to ensure effective adherence with applicable compliance laws and regulations

2. "Managers" through the directive issued by "Board" have elected the AML Officer to supervise the overall management of ZIPCO Remit's AML Program. This individual shall report directly to the Senior Management Officer so designated by the Board of Directors and be dully approved by the Board of Directors. On at least an annual basis, the CAMLO is to make a written report to the Board of Directors regarding the status of ZIPCO Remit's compliance activities with respect to the AML Program and its guidelines, procedures and reporting.

   Specifically, the CAMLO is responsible for:

Performing a risk assessment to determine all areas of ZIPCO Remit where money laundering or terrorist financing may be created and provide a report to Senior Management. This risk assessment is to include:

i. An increased focus on ZIPCO Remit's operations (products, services, customers and geographic locations) that are more vulnerable to abuse by money launderers and other criminals; and

ii. The environment with which ZIPCO Remit operates and the activity in its marketplace.

B. Ensuring that adequate controls are in place before new products are offered;

C. Informing Management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious activity reports filed;

D. Providing the program continuity despite changes in management or employee composition or structure;

E. Maintaining all regulatory recordkeeping and reporting requirements, recommendations for AML compliance and providing timely updates in response to changes in regulations;

F. Implementing and reviewing any related policies and procedures to ensure compliance with ZIPCO Remit's AML Program requirements;

G. Providing adequate controls for higher risk customers, transactions and products as necessary, such as transaction limits or management approvals;

H. Enabling the timely identification of reportable transactions and ensure accurate filing of required reports;

I. Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the AML Program;

J. Incorporating AML compliance into job descriptions and performance evaluations of appropriate personnel;

K. Training ZIPCO Remit personnel on AML Program directives; and

L. Supporting an independent AML audit program

3. Compliance Committee. The Compliance Committee to provide assistance to and support the CAMLO to promote effective management of ZIPCO Remit's AML Program

Specifically, the Board of Directors is responsible for:

A. Assisting the CAMLO in ensuring the compliance mandate established by this policy is an integral part of ZIPCO Remit operations;

B. Ensuring the Board of Directors is informed of ZIPCO Remit's compliance efforts on a periodic basis;

C. Providing guidance to the CAMLO to ensure ZIPCO Remit adapts to changes mandated by the law.

D. Reviewing and approving ZIPCO Remit's AML Program training program;

E. Providing assistance to the AML Officer with the responses to audit exceptions and/or regulatory examination results; and

F. Providing overall general guidance and expertise to ensure the successful implementation of ZIPCO Remit's AML Program

4. Risk Analysis and Assessment

ZIPCO Remit, as part of its AML Program, shall conduct a risk analysis to identify specific criteria of potential money laundering risks. This risk-based approach includes the identification of the money laundering and terrorist financing risks (to the extent that such terrorist financing risk can be identified) of customers, categories of customers, and transactions that allow ZIPCO Remit to determine and implement proportionate measures and controls to mitigate these risks.

ZIPCO Remit measures money laundering and terrorist financing risks using the following categories. The application of risk categories provides a strategy for managing potential risks by enabling ZIPCO Remit to subject customers to proportionate controls and oversight. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary depending on ZIPCO Remit's unique circumstances.

A. **Country or Geographic Risk**. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Factors that may result in a determination that a country poses a higher risk include: Countries subject to sanctions, embargoes or similar measures issued by the United Nations ("UN") as an example. In addition, some circumstances subject countries to sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized, may be given credence by ZIPCO Remit because of the standing of the issuer and the nature of the measures;

B. Countries identified by credible sources as lacking appropriate AML laws, regulations and other measures. The term "credible sources" refers to information that is produced by well-known bodies that are generally regarded as reputable and that make such information publicly and widely available.

In addition to Canadian Financial Action Organizations other sources may include, but are not limited to, supra-national or international bodies such as the **International Monetary**

Fund, the World Bank and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organizations.
Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them; or

C. Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

1. Customer Risk. Determining the potential money laundering or terrorist financing risks (to the extent that such terrorist financing risk can be identified) posed by a customer or category of customers is a critical component. Based on its own criteria, ZIPCO Remit is able to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. The application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include:

   A. Customers conducting their business relationship or transactions in unusual circumstances, such as:
      i. Significant and unexplained geographic distance between ZIPCO Remit and the location of the customer;
      ii. Frequent and unexplained movement of accounts to different institutions; and
      iii. Frequent and unexplained movement of funds between institutions in various geographic locations.
   B. The structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests of the customer
   C. Cash (and cash equivalent) intensive businesses including:
      i. Money services businesses (e.g. remittance houses, currency exchange houses, money transfer agents and bank note traders or other businesses offering money transfer facilities or services);
      ii. Casinos, betting and other gambling related activities; and
      iii. Businesses that while not normally cash intensive generate substantial amounts of cash for certain transactions.
   D. Charities and other “not for profit” organizations which are not subject to monitoring or supervision (especially those operating on a “cross border” basis).
   E. "Gatekeepers" such as accountants, lawyers, or other professionals holding accounts at ZIPCO Remit, acting on behalf of their clients/cardholders, and when ZIPCO Remit places

Un-reasonable reliance on the gatekeeper.

F. Use of intermediaries within the relationship who are not subject to adequate AML laws and measures and who are not adequately supervised

G. Customers that are Politically Exposed Persons (PEPs).

H. Services identified by competent authorities or other credible sources as being potentially higher risk, including, for example:

   i. International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank) and pouch activities; and

   ii. International private banking services

I. Services involving banknote and precious metal trading and delivery; or

J. Services that inherently have provided more anonymity or can readily cross international borders, such as online banking, stored value cards, international wire transfers, private investment companies and trusts

2. Other Risk Variables. ZIPCO Remit risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include the:

   A. Product and Service Risk. This category of risk includes the determination of potential risks presented products and services offered by ZIPCO Remit, such as risks associated with new or innovative products or services and the following factors:

   B. Services identified by competent authorities or other credible sources as being potentially higher risk, including, for example:

   C. International correspondent banking services involving transactions such as commercial payments for non-customers (for example, acting as an intermediary bank) and pouch activities; and

   D. International private banking services

   E. Services involving banknote and precious metal trading and delivery; or

   F. Services that inherently have provided more anonymity or can readily cross international borders, such as online banking, stored value cards, international wire transfers, private investment companies and trusts

3. Other Risk Variables. ZIPCO Remit's risk-based approach methodology may take into account risk variables specific to a particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction and may include the:

A. Purpose of an account or relationship which may influence the assessed risk. Accounts opened primarily to facilitate traditional, low denominated consumer transactions may pose a lower risk than an account opened to facilitate large cash transactions from a previously unknown commercial entity.

B. Level of assets to be deposited by a particular customer or the size of transactions undertaken. Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a customer that would otherwise appear to be higher risk might allow ZIPCO Remit to treat the customer as lower risk.

C. Level of regulation or other oversight or governance regime to which a customer is subject. A customer that is a financial institution regulated in a country with a satisfactory AML regime poses less risk from a money laundering perspective than a customer that is unregulated or subject only to minimal AML regulation.

D. Regularity or duration of the relationship. Long standing relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering perspective.

E. Familiarity with a country, including knowledge of local laws, regulations and rules, in addition to the structure and extent of regulatory oversight, as the result of ZIPCO Remit's own operations within the country.

F. Use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily increases the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

5. Risk Mitigation Strategies

ZIPCO Remit shall implement the following risk mitigation strategies:
Customer Identification, Due Diligence and Know Your Customer. ZIPCO Remit has implemented a Customer Identification Program (CIP) that enables personnel to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake:

A. Identifies and verifies the identity of each customer on a timely basis;

B. Takes reasonable risk-based measures to identify and verify the identity of any beneficial owner;

C. Obtains appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions;

D. Assesses the risks that the customer may pose taking into consideration any appropriate risk variables before making a final determination. This due diligence process includes:

1. A standard level of due diligence that is applied to all customers when initiating or continuing a relationship, such as:
   i. Evaluating the nature of the relationship. As an example, determining the length of a customer's relationship with ZIPCO Remit, the products and services provided to a customer, and the manner in which a customer was referred to ZIPCO Remit. The nature of a customer's relationship may serve to mitigate or to increase the overall risk indicators described below.
   ii. Identifying high risk geographies, including customers located in or conducting business transactions in High Risk Money Laundering and Related Financial Crime Areas; and
   iii. Identifying high risk entities, banking functions and transactions (refer to the High-Risk Entities subtopic below).
2. The standard level being reduced in recognized lower risk scenarios, such as:
   i. Publicly listed companies subject to regulatory disclosure requirements;
   ii. Other financial institutions (domestic or foreign) subject to an AML regime consistent with all AML recommendations;
   iii. Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds; or
   iv. Transactions involving the minimum amounts for particular types of transactions (e.g. small insurance premiums).
3. The standard level being increased with respect to customers that are determined to be of higher risk due to the nature of their activities which may require increased monitoring.

   This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as correspondent ZIPCO Remitting relationships and PEPs. These enhanced due diligence procedures include, but are not limited to:
   i. Increased awareness by ZIPCO Remit personnel of higher risk customers and transactions within business lines across ZIPCO Remit;
   ii. Increased levels of ZIPCO Remit's CIP, Know Your Customer (KYC), and enhanced due diligence;

iii. Appropriate additional documentation is obtained to confirm the identity and lawful business activities of a customer;

iv. Escalation for approval of the establishment of an account or relationship;

v. An understanding of the normal and expected transactions of a customer, including increased monitoring of transactions;

vi. Increased levels of ongoing controls and frequency of reviews of relationships; and

vii. Reporting of suspicious activities in compliance with existing reporting requirements

1. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA")

In accordance with the prescribed legislative requirements, our ZIPCO Remit has to fulfill certain record keeping, identification, and reporting requirements. Our ZIPCO Remit has chosen to implement and maintain a compliance regime which includes:

- AML Program oversight from the Chief Anti-Money Laundering Officer ("CAMLO");
- The development and implementation of compliance policies and procedures;
- Executing Know Your Customer ("KYC") procedures on all customers;
- An assessment of our risks as it relates to money laundering and terrorist financing;
- Monitor transactions for potentially suspicious and attempted suspicious activities for the purposes of filing Suspicious Transaction Reports ("STR");
- Maintaining and providing written, ongoing compliance training for our employees to ensure their understanding of their responsibilities under the Proceeds of Crime Act and Regulations in Canada; and,
- A periodic review of our compliance regime to test its effectiveness related to money laundering and terrorist financing every two years.

Monitoring of Customers and Transactions.

The degree and nature of monitoring performed by ZIPCO Remit is based upon its size, the AML risks that ZIPCO Remit has identified, the monitoring method being utilized (manual and/or automated), and the type of activity under scrutiny. Not all transactions, accounts or customers are monitored in the same way.

1. The degree of monitoring is based on the perceived risks associated with a customer, the products or services being used by the customer, and the location of the customer and the transactions. In any respect, such monitoring is appropriately documented.

The principal of ZIPCO Remit's risk-based monitoring system is to respond to enterprise wide issues

based on ZIPCO Remit's analysis of its major risks. Monitoring under this risk-based approach allows ZIPCO Remit to create monetary or other thresholds below which an activity will not be reviewed. Defined situations or thresholds used for this purpose are reviewed on a regular basis to determine adequacy for the risk levels established. In addition, adequacy of any systems and processes are assessed on a periodic basis by Senior Management and appropriately documented.

2. **Suspicious Transaction Reporting**- The regulatory and legal requirement to report suspicious transactions or activity by ZIPCO Remit provides federal authorities the ability to utilize such financial information to combat money laundering, terrorist financing and other financial crimes. When a legal or regulatory requirement mandates the reporting of suspicious activity once a suspicion has been formed, a report must be made by ZIPCO Remit. Therefore, a risk-based approach for the reporting of suspicious activity under these circumstances is not applicable.
3. However, a risk-based approach is appropriate for the purpose of identifying suspicious activity (such as directing additional resources at those areas ZIPCO Remit has identified as higher risk). In the same respect, ZIPCO Remit uses information provided by state and federal authorizes to enhance its approach for identifying suspicious activity. In addition, Management should always periodically assess the adequacy of ZIPCO Remit's system employees training and assessment for identifying and reporting suspicious transactions.

4. **Training and Awareness-** ZIPCO Remit provides its employees with AML Program training that is appropriate and proportional with regard to money laundering and terrorist financing for their respective positions. This enterprise wide effort provides all relevant employees with general information on AML laws, regulations and internal policies that is:

   A. Tailored to the appropriate staff responsibility (e.g. customer contact or operations);
   B. At the appropriate level of detail (e.g. front-line personnel, complicated products or customer managed products);
   C. At a frequency related to the risk level of the business line involved; and
   D. Tested to assess knowledge commensurate with the detail of information provided.

6. Money Laundering and Terrorist Financing Red Flags

The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all inclusive, they are designed to help ZIPCO Remit personnel to recognize possible money laundering and terrorist financing schemes. The mere presence of a red flag is not by itself evidence of criminal activity. ZIPCO Remit personnel are to use closer scrutiny to help determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

1. Customers Who Provide Insufficient or Suspicious Information.

   A. A customer uses unusual or suspicious identification documents that cannot be readily verified.

   B. A customer provides an individual tax identification number after having previously used a Social Security number.

   C. A customer uses different tax identification numbers with variations of his or her name.

   D. A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior ZIPCO Remitting relationships, the names of its officers and directors, or information on its business location.

   E. A customer's home or business telephone is disconnected.

   F. The customer's background differs from that which would be expected on the basis of his or her business activities.

   G. A customer makes frequent or large transactions and has no record of past or present employment experience.

   H. A customer is a trust, shell ZIPCO Remit, or private investment ZIPCO Remit that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open ZIPCO Remit accounts for those shell companies while shielding the owner's identity.

2. Efforts to Avoid Reporting or Recordkeeping Requirements.

   A. A customer or group tries to persuade a ZIPCO Remit employee not to file required reports or maintain required records.

   B. A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.

   C. A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

   D. A business or customer asks to be exempted from reporting or recordkeeping requirements.

a) A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as non-cooperative countries and territories).

---

1. Funds Transfers

A. Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.

B. Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.

C. Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.

D. Large, incoming funds transfers are received on behalf of a foreign client/cardholder, with little or no explicit reason.

E. Funds transfer activity is unexplained, repetitive, or shows unusual patterns.

F. Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

E. Funds transfers are sent or received from the same person to or from different accounts.

F. Funds transfers contain limited content and lack related party information.

G. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high risk locations.

H. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

I. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.

J. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

K. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high risk countries.

3. Electronic Funds Transfer

   A. Large value, automated clearing house (EFT) transactions are frequently initiated through third party service providers (TPSP) by originators that are not ZIPCO Remit customers and for which ZIPCO Remit has no or insufficient due diligence.
   B. TPSPs have a history of violating EFT network rules or generating illegal transactions or processing manipulated or fraudulent transactions on behalf of their customers.
   C. Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.
   D. Unusually high level of transactions initiated over the Internet or by telephone.

4. Activity Inconsistent with the Customer's Business
   A. The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
   B. Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals
   C. Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high risk countries (e.g., countries designated by national authorities as non-cooperative countries and territories).
   D. The stated occupation of the customer is not commensurate with the type or level of activity
   E. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
   F. With respect to nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction

5. Employees

   A. Employee exhibits a lavish lifestyle that cannot be supported by his or her salary. TPSPs have a history of violating EFT network rules or generating illegal transactions or processing manipulated or fraudulent transactions on behalf of their customers.
   B. Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
   C. Employee is reluctant to take a vacation.

7. Detection and Monitoring Procedures

ZIPCO Remit follows these policies and procedures that are implemented for the detection and prevention of money laundering activities as part of Zip Coin Remit's AML Program:

1. Monitoring suspected money laundering transactions via ZIPCO Remit's money laundering report produced by ZIPCO Remit's host system computer. The CAMLO is responsible for reviewing this report on a weekly and monthly basis to detect possible instances of money laundering activity.

   The CAMLO is to print and maintain reports produced by the system to substantiate his opinion that specific activity is, or is not, suspicious;

2. Identifying high risk activities, businesses and foreign countries (those associated with money laundering);

3. Identifying and monitoring non-financial institutions that are clients of ZIPCO Remit and that engage in high volumes of cash activities (i.e., money transmitters and check cashing businesses);

4. Being aware that new customers are expected to live or work near an office of ZIPCO Remit. Customers that do not meet the residency requirement are to be asked to explain why they choose to bank with ZIPCO Remit. Failure to provide a sufficient explanation should be grounds for denying the account to be opened;

5. Being aware of customers that open a new account (prepaid card) with $5,000 or more in cash. Customers who do are to be asked to substantiate the legitimacy of the funds;

6. Being aware of customers that are making deposits of $3,000 or more in a day, or $5,000 or more in a week on to their account. Customers conducting such activity are to be asked to substantiate the legitimacy of the funds. A customer's card account is to be closed if a customer cannot provide sufficient proof of his or her activity;

7. Reporting customers that asked to be excluded from Currency Transaction Reporting (CTR) reporting to FINTRAC (via a Suspicious Activity Report - SAR) in addition to their account being closed;

8. Reporting customers that refuse to provide necessary information for filing a CTR to FINTRAC (via a SAR) in addition to their account being closed;

9. Monitoring business accounts by identifying the following activities:

A. One or more online remit transfers a week, which are structured, avoid CTR reporting. (Note: a payment from a debit card or wire transfer is considered structured if it is between $8,000 and $10,000);

B. Two or more instances a week, where a customer makes two or more online transfers on the same day, and the total of the deposits is between $5,000 and $8,000;

C. One or more instances a week, where a customer has made online transfers to two or more related accounts, and the total transfers is between $5,000 and $10,000;

D. Online transfers that are over $10,000, and, that are 25% greater than the customer's second highest cash deposit; (not applicable if over card limit)

E. Online transfers that are over $10,000, and, that are 150% of the customer's average cash deposits (ignoring inconsequential deposits that are below $3,000);

ZIPCO Remit procedures for compliance are as follows:

1. Record Search Procedures. Upon receiving an information request from FINTRAC as described above, the AMLO is to search ZIPCO Remit's records to determine whether ZIPCO Remit maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FINTRAC's request.

2. The AML Officer should contact the Federal law enforcement agency named in the information request provided to the institution by FINTRAC with any questions relating to the scope or terms of the request. Except as otherwise provided in the information request, ZIPCO Remit is only required to search its records for:

   A. Any current account maintained for a named suspect;

   B. Any account maintained for a named suspect during the preceding twelve months; and

   C. Any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmitter or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution

3. Report to FINTRAC. If the CAMLO identifies an account or transaction identified with any individual, entity, or organization named in a request from FINTRAC, it shall report to FINTRAC, in the manner and in the time, frame specified in FINTRAC's request, the following information:

   A. The name of such individual, entity, or organization;

   B. The number of each such account, or in the case of a transaction, the date and type of

each such transaction; and

C. Any Social Insurance number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened, or each such transaction was conducted.

4. Designated Contact Person. The CAMLO is the point of contact for ZIPCO Remit for such investigative issues or similar requests for information from FINTRAC.

5. Use of Security Information. It is against ZIPCO Remit policy to use information provided by FINTRAC in an investigation for any purpose other than:
   A. Reporting to FINTRAC;
   B. Determining whether to establish or maintain an account, or to engage in a transaction; or
   C. Assisting ZIPCO Remit in complying with this requirement.

   Additionally, ZIPCO Remit may not disclose to any person, other than FINTRAC or the Federal law enforcement agency on whose behalf FINTRAC is requesting information, the fact that FINTRAC has requested or has obtained information under this section, except to the extent necessary to comply with such an information request. However, ZIPCO Remit is authorized to share information concerning an individual, entity, or organization named in a request from FINTRAC in accordance with this policy. Such sharing shall not disclose the fact that FINTRAC has requested information concerning such individual, ZIPCO Remit entity, or organization that FINTRAC requires more detail and documents.

   It is the policy of ZIPCO Remit to maintain adequate procedures to protect the security and confidentiality of requests from FINTRAC.

6. No Other Action. It is against ZIPCO Remit policy to take any action, or to decline to take any action, with respect to an account established for, or a transaction engaged in with, an individual, entity, or organization named in a request from FINTRAC, or to decline to establish an account for, or to engage in a transaction with, any such individual, entity, or organization. Except as otherwise provided in an information request, such a request shall not require ZIPCO Remit to report on future account opening activity or transactions or to treat a suspect list received as described by the regulation

8. Information Sharing with Other Financial Institutions

ZIPCO Remit, under the protection of the safe harbor from liability, may voluntarily receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects

may involve possible terrorist activity or money laundering.

The following rules apply:

1. Notice Requirement. ZIPCO Remit or another financial institution that intends to share information is to submit to FINTRAC a “Notice for Purposes. Each notice provided is effective for the one year period beginning on the date of the notice.

   In order to continue to engage in the sharing of information after the end of the one year period, ZIPCO Remit must submit a new notice. The CAMLO is responsible for completing and submitting the notice to FINTRAC for ZIPCO Remit on an annual basis.

2. Verification Requirement. Prior to sharing information, it is the responsibility of the CAMLO to take reasonable steps to verify that the financial institution with which ZIPCO Remit intends to share information has submitted to FINTRAC their notice. Verification may be obtained by confirming that the other financial institution appears on a list that FINTRAC will periodically make available to ZIPCO Remit that have filed a notice with it, or by contacting FINTRAC directly to ensure the notice has been filed.

3. Use of Information. It is against ZIPCO Remit policy for information received from another financial institution be used for any purpose other than:

   A. Identifying and, where appropriate, reporting on money laundering or terrorist activities
   B. Determining whether to establish or maintain an account, or to engage in a transaction; or
   C. Assisting a financial institution in complying with the regulation.

4. Safe Harbor Liability. If ZIPCO Remit shares information with another financial institution it is protected from liability for such sharing, or for any failure to provide notice of such sharing, to an individual, entity, or organization that is identified in such sharing, to the full extent provided by law.

5. Information Sharing Between Financial Institution and the Federal Government. If, as a result of information shared by ZIPCO Remit, and ZIPCO Remit knows, suspects, or has reason to suspect that an individual, entity, or organization is involved in, or may be involved in terrorist activity or money laundering, and ZIPCO Remit is subject to a suspicious activity reporting, the CAMLO is to file a Suspicious Activity Report. In situations involving violations requiring immediate attention, such as when a reportable violation involves terrorist activity or is ongoing, the AML Officer is to immediately notify, by telephone, an appropriate law enforcement authority and Senior Management in addition to filing a Suspicious Activity Report.

It is the intent and policy of ZIPCO Remit to have a clear and concise understanding of all customer practices in order to avoid criminal exposure by any "customer" who would use ZIPCO Remit's resources for illicit purposes.

b) ZIPCO Remit's Chief Anti-Money Laundering Officer

Under the PCMLTFA, ZIPCO Remit has designated a CAMLO- **Kim Chivhima** who is responsible for the implementation and oversight of our compliance regime. The CAMLO has the authority and the resources to ensure the ongoing compliance of our organization as it relates to the identification and prevention of money laundering and terrorist financing.

c) Ongoing Monitoring of Business Relationships

As per FINTRAC Guidance, business relationships are If necessary, we may require our clients to provide additional documentation or information to confirm source of funds or the purpose of the transaction.

ZIPCO Remit's compliance staff will review any transactions that trigger an alert and determine if the transactions are within the clients' stated activity before being released or completed. In some cases, ZIPCO Remit will require additional information from the client such as source of income, proof of employment, nature of the client's business, as well as review of client's transaction history.

d) Record Keeping

As a registered MSB with FINTRAC, ZIPCO Remit is required to keep certain types of records depending on the client type and transaction type - this includes records of any STR's submitted to FINTRAC. There is no threshold (that is, no dollar amount) for a suspicious transaction. When we have to send an STR to FINTRAC, we must take reasonable measures, before the transaction is reported, to ascertain the identity of the individual who conducted or attempted to conduct the transaction.

We are required to maintain an effective recordkeeping system to enable FINTRAC to have access to the records in a timely fashion. Our records have to be kept for a minimum of 7 years, and in such a way that they can be provided to FINTRAC within 30 days of a request to examine them.

8.1 How to identify individual clients

Prior to a client being able to perform a transaction, ZIPCO Remit must identify that client in accordance with applicable regulations. ZIPCO Remit has a policy which requires all customers to be "verified" prior to being able to undertake any form of transactions through our remitting platform. Accounts are only verified and validated via ZIPCO Remit system in order to mitigate issues against the risk of money laundering and terrorist financing activities.

8.2 Data acquisition and Identity Verification Process

ZIPCO Remit requires particular information from the end-users or clients (depending on whether it is an on-site or off-site verification) in order to perform Identity and document verification services. ZIPCO Remit handles all instant verification for KYC and AML. Personally, Identifiable Information (PII Data) is collected, which includes name, contact information (email ID and phone number), DoB and any other information required to carry out the verification checks. For instance, if the client selects the Face Verification service, we will also collect the image (selfie) or video (short clip showing user's face) proof from the user. If end user opts for document verification, then we would require an image or video of the desired document from bot, the front and the back side of the document.

Future Enhancement

For AML Screening service, ZIPCO Remit will require the user's Name and DoB for running them against the AML databases, sanctions, and watchlists. ZIPCOIM- our Identity Verification Process describes what information we collect, how we collect it and when we collect it. For more information ZIPCO Remit website can be accessed here: https://zipcoinremit.com

8.3 Our End-users

The end-users are ZipCoin's customers, whose identities are being verified; and documents we authenticate and run against AML lists and databases. We have chosen the onsite ID verification; our customers are redirected to our ZIPCOIM website and we directly collect end-user's verification data from the end-users themselves. This data includes but is not limited to the images/videos of the end user's identity documents (e.g. passport, ID card, driving license or credit/debit card), their biometric facial identifiers (e.g. face images/videos). ZipCoin also require textual information that is either extracted directly from the end-user's identity particulars or is provided by the end-user at each step. In the latter case, that data is compared to the information present on the identity particulars, using the template matching and computer vision-based techniques. If the face image of the end-user is compared to the photograph present on their identity documents, using facial recognition mechanism. By screening the end-user against the AML lists and databases, ZIPCO Remit ensures that we don't let through no fraudster, criminal, imposter, or any person associated or convicted of the cybercrime, helping us further combat breaches, violations, and infraction of intellectual property laws.

8.4 Manual Verification (Dual process method)

This method involves referring to information from reliable and independent sources which can be submitted by the individual in original paper form or in electronic form. As part of the account sign up process, our clients are asked to upload to our site the original electronic or paper documents they received or downloaded. All documents must be valid and unaltered in order to be acceptable. If any information has been redacted, it is not acceptable.

8.6 How to Identify Corporations and Other Entities

For corporate clients, we are required to confirm the existence of the entity, and the entity's beneficial ownership.

(1) Corporations

We confirm the existence of a corporation as well as the corporation's name and address, by referring to the following documents:

- Power to bind the corporation - Articles of incorporation (with full names of all Directors and at least 3 Authorized Signatories (if any))
- Proof of existence:
  - Certificate of Corporate Status (if incorporated within the previous 12 months);
  - Corporation Profile Report;
  - A record that has to be filed annually under provincial securities legislation;
  - Corporation's published annual report signed by an independent audit firm; or
  - A letter or a notice of assessment from a municipal, provincial, territorial or federal government.
- Proof of address (utility bill, bank statement or any government record) - if not in the first or second bullet above
- Trade name registration, if applicable
- Beneficial Ownership Attestation (BOA) form and ID of the ultimate beneficiary including the names and addresses of the individuals who are the beneficial owners (i.e. any actual person who owns or controls, directly or indirectly, 25% or more of the corporation's shares). If an individual beneficial owner does not exist, ZIPCO Remit will apply the necessary measures to mitigate the risk.
- Signed Corporate Resolution

- The completed ZIPCO Remit signup form (including the nature of business, source of funds and estimated transaction volumes, as well as any enhanced due diligence measures deemed necessary and as requested)

(2) Entities other than a corporation

We confirm the existence of an entity other than a corporation by referring to a partnership agreement, articles of association or any other similar record that confirms the entity's existence.

In confirming an entity's existence, we must be able to refer to a paper or electronic record and retain a copy of it. Verbal confirmation is not sufficient. Electronic records must be from a public source and we must record the type and source and corporation's registration number.

(3) Not-for-profit organization

If the entity is a not-for-profit organization, we also have to do the following:

- Determine whether or not the entity is a registered charity for income tax purposes
- If that entity is not a registered charity, determine whether or not it solicits charitable financial donations from the public

(4) Beneficial Ownership Records

In addition to confirming the existence of a corporation or other entity, we also must also determine and confirm the accuracy of the entity's beneficial ownership through the following:

- If the entity is a corporation:
  - The name and occupation of all directors and officers of the corporation; and
  - The name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation.
- If the entity is other than a corporation:
  - The name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the entity.

(5) Keeping Client Identification Information Updated

ZIPCO Remit clients who present an elevated risk will have their client identification information updated at least every two years, or sooner depending on our evaluation. Clients who present an

elevated risk include (but is not limited to) Politically Exposed Persons ("PEPs") in all of its legal forms. This is to be done by reviewing original identity or entity documents and recording the updated identification or information details for our files as appropriate.

f) Suspicious Transaction Reports

ZIPCO Remit must report any transactions or attempted transactions where there are reasonable grounds to suspect it relates to money laundering or terrorist activity. There is no monetary threshold for submitting a Suspicious Transaction Report.

The CAMLO has the authority to file STRs with FINTRAC and is required to maintain a log of all reports filed in accordance with ZIPCO Remit's record keeping procedures.

'Reasonable grounds to suspect' captures predicate offences and that tax evasion is also considered a predicate offence for money laundering. Accordingly, if we suspect transactions are being undertaken to avoid or evade paying income taxes, ZIPCO Remit is obligated to report the transactions as suspicious to FINTRAC.

g) Terrorist Property Reporting and Sanctions Requirements

There are two situations where we must send a terrorist property report to FINTRAC immediately:

- Knowing that a property is owned or controlled by or on behalf of a terrorist or terrorist group; and,
- Believing that a property is owned or controlled by or on behalf of a listed person.

Where there are economic sanctions, ZIPCO Remit is required to prohibit or restrict activities in accordance with the legal requirements. In some cases, ZIPCO Remit may be required to freeze property, in addition to making reports to various government and law agencies.

h) Ongoing Monitoring of Business Relationships

If in the course of reviewing and monitoring, we identify unexplainable or unusual patterns or activity, we will work to obtain further information so that these questions are satisfactorily answered. ZIPCO Remit may also report the activity internally to the CAMLO who is required to maintain a record/log of all internally reported and perform a review to determine if an STR is to be filed with FINTRAC.

If ZIPCO Remit cannot reach a clear understanding of the client's identity, or the sources and movement of funds, it may result in the account being permanently closed. This will be followed by terminating the relationship and de-marketed account owner without the right of re-opening a new account.

The objective of this policy is to ensure the immediate detection and identification of suspicious activity.

The Compliance Officer for this policy is **Cathrine (Kim) Chivhima**. The responsibility of the Compliance Officer is to ascertain that Company policy is in compliance with the current laws and regulations, and that the policy is communicated to the appropriate employees and agents.

All employees and agents have been provided with a copy of this policy. All new employees and agents will be provided with a copy of this policy at their time of hiring. It will be the responsibility of all "Managers" to provide ongoing training regarding this policy and the procedures for compliance.

We appreciate your understanding and full cooperation in implementing this policy.

Management approved this policy on April 15th, 2019

Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

www.**fintrac**.gc.ca/ for further help and understanding


ZPCOIN
REMIT