ONYX GLOBE PAYMENT LTD.
January 4, 2021

AML Policy

Purpose

This document sets out the principles and standards for compliance and management of risks associated with financial crime in ONYX GLOBE PAYMENT LTD. The purpose of this document is to prevent the ONYX GLOBE PAYMENT LTD from being used for financial crime to comply with all applicable legal requirements and to ensure that the most appropriate action is taken by the ONYX GLOBE PAYMENT LTD to mitigate the risks associated with financial crime.

This document outlines the applicable legal requirements related to financial crime to which the ONYX GLOBE PAYMENT LTD must adhere, as well as internal measures which are established by the ONYX GLOBE PAYMENT LTD to ensure it complies with these legal requirements. This document is referred to as the Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), Counter-Proliferation Financing (CPF) and Sanctions Policy (the Policy) and sets the parameters for the ONYX GLOBE PAYMENT LTD in relation to the AML, CTF, CPF and sanctions framework.

Scope and application

The Policy applies to all ONYX GLOBE PAYMENT LTD employees, all units in the ONYX GLOBE PAYMENT LTD, senior management, foreign correspondents, contractors and third parties with whom ONYX GLOBE PAYMENT LTD may contract with.

The aim of the ONYX GLOBE PAYMENT LTD is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the ONYX GLOBE PAYMENT LTD of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity.

The Policy is updated at least once a year, or more frequently based on international requirements and legislative changes, particularly with the implementation of the Canadian Payments Act, Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) or Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTF Regulations) and associated Regulations or Financial Transactions and Reports Analysis Centre (FINTRAC) Guidance on the Risk-Based Approach and Compliance program requirements.

Definitions

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- Placement: Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial institutions.
- Layering: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
- Integration: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

It also covers money, however acquired, which is used to fund terrorism. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Terrorist financing relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism or with the intention to dispose those funds to a terrorist group or a separate terrorist.

Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Criminal property is the proceeds of criminal conduct. This includes any type of conduct, wherever it takes place, which would constitute a criminal offence if committed in ONYX GLOBE PAYMENT LTD. It includes drug trafficking, terrorist activity, tax evasion, corruption, fraud, forgery, theft, counterfeiting, black mail and extortion. It also includes any other offence that is committed for profit.

Sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security. Sanctions can be:

a) Specific, i.e. relate to specific lists of named individuals, legal entities, organizations, vessels etc. (for example the US Department of Treasury refers to some of these entities as Specially Designated Nationals),

b) General, i.e. cover all transactions with certain countries or jurisdictions; certain transactions with countries or jurisdictions such as exports, imports or new investment, or all transactions within a certain area of activity/products (for example arms sales to a particular country).

c) Sectoral, i.e. cover certain parties in specific sectors (for example OFAC designates parties on a Sectoral Sanctions Identification List or "SSI List") but only restrict certain transactions of these designated parties.

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

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) must establish an AML/ATF compliance program. The PCMLTF Regulations set out specific requirements, including:

- the appointment of a person responsible for the compliance program;
- the development and application of compliance policies and procedures that are up to date and approved by a senior officer;
- a program to assess the risk of a money laundering or terrorist financing offence being conducted through the firm, and implementation of measures to mitigate high-risk scenarios;
- an ongoing written compliance training program for employees of the ONYX GLOBE PAYMENT LTD;
- a review of policies and procedures to test their effectiveness to be conducted every two years by an internal or external auditor;

PCMLTFA and latest redaction of FATF recommendations set out the requirement for relevant businesses to establish and maintain appropriate and risk-sensitive policies and procedures relating to:

- Customer due diligence
- Reporting
- Record keeping
- Internal control
- Risk assessment and management (Risk Based Approach)
- The monitoring and management of compliance, and

- The internal communication of such policies and procedures, in order to prevent activities related to money laundering and terrorist financing and proliferation financing.

These policies and procedures must:

- Identify and scrutinise
  - Complex or unusually large transactions
  - Unusual patterns of transactions which have no apparent economic or visible lawful purpose
  - Any other activity which could be considered to be related to money laundering or terrorist financing or proliferation financing
- Specify the additional measures that will be taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing
- Determine whether a customer is a politically exposed person (see Annex 5 for definition and further guidance)
- Nominate an individual in the organisation to comply with, and receive disclosures under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.
- Ensure employees report suspicious activity to the Nominated Officer, and
- Ensure the Nominated Officer considers such internal reports in the light of available information and determines whether they give rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

The main principles encompassed by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations can be described as Risk Based Approach (RBA). RBA requires several steps to be taken to determine the most cost-effective and proportionate way to manage and mitigate the money laundering and terrorist financing and proliferation financing and sanctions violation risks faced by the business. The steps are to:

- Identify the money laundering and terrorist financing and proliferation financing and sanctions violation risks that are relevant to the business
- Assess the risks presented by the particular:
  - Customers – types and behavior;
  - Products and services;
  - Delivery channels, for example, cash over the counter, electronic, wire transfer or cheque;
  - Geographical areas of operation, for example, location of business premises, source or destination of customers' funds;
  - Complexity and volume of transactions;
- Design and implement controls to manage and mitigate these assessed risks
- Monitor and improve the effective operation of these controls and
- Record appropriately what has been done, and why

Please see Annex 1 for detailed explanation of Risk Based Approach.

Where can I find more information?

Check out the following website that contain the details of different issues discussed in this document and is likely to be useful during your time with us:

1. Financial Transactions and Reports Analysis Centre (FINTRAC): https://www.fintrac-canafe.gc.ca
2. The Office of the Superintendent of Financial Institutions (OSFI): https://www.osfi-bsif.gc.ca

3. Financial Consumer Agency: https://www.ca/en/financial-consumer-agency.html
4. Financial Action Task Force (FATF): www.fatf-gafi.org
5. Office of Foreign Assets Control (OFAC): www.treasury.gov/ofac
6. The Financial Crimes Enforcement Network (FinCEN) advisory list: www.fincen.gov

Terms

These are terms you should be familiar with.

Terms/Acronyms	Definition
Nominated Officer	A Nominated Officer (also known as the MLR officer or AML Compliance Officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues.
Supporting Officer	A person or persons nominated to act on behalf of the Nominated Officer.
AML	Anti-Money Laundering
KYB	Know Your Business
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
FINTRAC	Financial Transactions and Reports Analysis Centre
PEP	Politically Exposed Persons
STR	Suspicious Transaction Report
RCMP	Royal Canadian Mounted Police
CSIS	Canadian Security Intelligence Service
SWIFT	Society for Worldwide Interbank Financial Telecommunications
OFAC	Office of Foreign Assets Control
FATF	Financial Action Task Force
FinCEN	The Financial Crimes Enforcement Network
UBO	Ultimate Beneficial Owner
EU	The European Union
UN	The United Nations

RBA	Risk Based Approach
CTF	Counter-Terrorism Financing
CPF	Counter-Proliferation Financing
CRA	Revenue Agency
FCAC	Financial Consumer Agency

Our Products and Services

ONYX GLOBE PAYMENT LTD is focused on providing the Merchant Services or Payment Card Processing services for various e-commerce Merchants incorporated in Worldwide and doing business Worldwide in compliance with Code of Conduct for the Credit and Debit Card Industry in ONYX GLOBE PAYMENT LTD and other legal requirements. To manage our risk effectively and fulfill compliance and sanction lists all customers and their business will be checked in UN sanctions, Canadian National Sanctions List, OFAC Sanctions List, Visa Inc. and MasterCard Worldwide lists and programs etc.

Merchant Services

Merchant Services or payment card processing is the handling of electronic payment transactions for merchants. Merchant processing activities involve obtaining sales information from the merchant, receiving authorization for the transaction, collecting funds from the bank which issued the payment card and sending payment to the merchant.

The actual transfer of funds to the merchant or settlement will be performed in further way. At the end of each day, the merchant will generally review the days sales, credits and voids. After verifying this, the merchant will close his batch, or the batch will be closed automatically. This entails closing out the days sales and transmitting the information for deposit into ONYX GLOBE PAYMENT LTD platform, and then to the bank. The acquiring bank routes the transaction through the appropriate settlement system against the appropriate card-issuing bank.

The card-issuing bank then sends the money back through settlement system (Visa, MasterCard etc) for the amount of the sales draft, less the appropriate "interchange fee," to the acquiring bank's account. The acquiring bank then deposits the amount, less the "discount fee" to the ONYX GLOBE PAYMENT LTD segregated client bank account. ONYX GLOBE PAYMENT LTD then deposit the amount less the "discount fee" to the Merchant account once per 2-7 business days. Generally, within 24-72 hours, the merchants will have their money. ONYX GLOBE PAYMENT LTD may offer some low risk Merchants "next day funding."

The settlement procedure varies on the front end depending on the program the merchant is on. A hotel, travel or car rental agency may want to get a pre-approval before the customer checks in or uses the service. In ONYX GLOBE PAYMENT LTD, we have many pre-built programs that any merchant can request based upon their type of business.

E-Vouchers

An E-Voucher is an electronic stored value voucher that can be generated real-time from website. The voucher can then be redeemed by the user through merchant interfaces. Once redeemed, the value of the E-Voucher is transferred to the account with that merchant and funds are instantly available for use.

E-Vouchers can be used by merchants in any scenario which requires their customers to load value to their account, effectively allowing cash in the form of a purchased voucher to be loaded to that account. It can be used for loading payment cards, transferring money to an e-wallet, loading a gaming account online or any other account type that is integrated with the platform.

Internal Controls and Communication

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) requires businesses to have appropriate systems of internal control and communication in order to prevent activities related to money laundering and terrorist financing. In simple terms this means that businesses must ensure that management controls are put in place that will alert the relevant people in the business to the possibility that criminals may be attempting to use the business to launder money or fund terrorism or fund proliferation or violate sanctions, so as to enable them to take appropriate action to prevent or report it.

Systems of internal control and communication must be capable of identifying unusual or suspicious transactions or customer activity, of identifying transactions and business relationships specified in a direction issued by FINTRAC. ONYX GLOBE PAYMENT LTD must report suspicious transactions under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

The nature and extent of systems and controls that the business needs to put in place will depend on a variety of factors, including the:

- Degree of risk associated with each area of its operation
- Nature, scale and complexity of the business
- Type of products, customers, and activities involved
- Diversity of operations, including geographical diversity
- Volume and size of transactions
- Distribution channels.

Therefore, the ONYX GLOBE PAYMENT LTD has established internal controls procedure. The basis of the internal control process is well-defined authorisations, a segregation of duties, identification of clients, on-going due diligence, reporting suspicions, etc. The ONYX GLOBE PAYMENT LTD doesn't have an internal audit unit, however ONYX GLOBE PAYMENT LTD plans to carry out an auditing not less than once in two years, forming a group of three employees which are working in unrelated departments, unless it is assessed by the ONYX GLOBE PAYMENT LTD that a longer rotation cycle is appropriate. The decision of the participants of the formed group and the audit is made by the board of the company.

The ONYX GLOBE PAYMENT LTD regularly monitors changes in and compliance with relevant legislation and other legal requirements in order to mitigate money laundering and terrorism financing and proliferation financing and sanctions violation risks, as well as to make internal control procedures more efficient.

The Money Laundering Reporting Officer (Nominated Officer)

A Nominated Officer is the person within an organisation who is responsible for overseeing all activity related to anti-money laundering matters. Please familiarize yourself with the below personnel as you should be working closely with them.

Company's Nominated Officer is Name Surname

In the absence of the Nominated Officer, Supporting Nominated Officers will take his/her place.

Company's Supporting Nominated Officer is Name Surname

ONYX GLOBE PAYMENT LTD's Nominated Officers should remain up-to-date with AML/ATF rules and risks. If Nominated Officers deal with day-to-day regulatory issues, changes to AML/ATF requirements, they may not have enough time to maintain the knowledge needed to oversee an effective AML/ATF regime. If this is the case, the ONYX GLOBE PAYMENT LTD may want to consider designating a different qualified individual as the Nominated Officer.

The Nominated Officer's responsibilities include:

- Receiving disclosures from employees (also known as Suspicious Transaction Report - STR's).
- Deciding if disclosures should be passed on to the Financial Transactions and Reports Analysis Centre or the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS).
- Reviewing all new laws and deciding how they impact on the operational process of the company
- Preparing a written procedures manual and making it available to all staff and other stakeholders
- Making sure appropriate due diligence is carried out on customers and business partners
- Receiving internal Suspicious Transaction Report (STR) from staff
- Deciding which internal STR's need to be reported on to FINTRAC or RCMP or CSIS.
- Recording all decisions relating to STRs appropriately
- Ensuring staff receive anti-financial crime training when they join and that they receive regular refresher training
- Monitoring business relationships and recording reviews and decisions taken
- Making decisions about continuing or terminating trading activity with particular customers
- Making sure that all business records are kept for at least five years from the date of the last customer transaction as per FINTRAC regulations.

The Nominated officer is a person who has sufficient authority and autonomy in order to make the decisions required above. The Supporting Nominated Officer shall replace the Nominated Officer when he/she is unavailable.

Staff Training and Reporting

Training Policy

ONYX GLOBE PAYMENT LTD maintains an on-going employee training program so that the staff is adequately trained in KYC procedures and that the staff is aware of different possible patterns and

techniques of money laundering which may occur in their everyday business. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers/Merchants. New staff is educated in the importance of KYC policies and the basic requirements at the Company. Training is given to all staff members upon commencement of taking on the position in the ONYX GLOBE PAYMENT LTD and on regular occasions afterwards (at least once a year).

Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities or sanctions violation typologies.

Regular refresher training is provided to ensure that employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

Training covers the following issues:

- The law relating to financial crime;
- Risks associated with the financial crime threat to the company (see, for example, www.egmontgroup.org);
- Identity and responsibilities of the Nominated Officer;
- Internal policies and procedures put in place;
- Customer Due Diligence/Enhanced due diligence monitoring measures;
- Suspicious activity – what to look out for;
- How to submit an internal Suspicious Transaction Report to the Nominated Officer;
- Record-keeping requirements;
- Possible sanctions violation – what to look out for;

The Nominated Officer will keep a log of all training which is provided to staff members.

All staff will be required to sign the training log where required to confirm that they have received training.

The Nominated Officer will circulate to all staff other material to heighten awareness of anti-financial crime issues. This must be placed on the company notice board which should be available in all company's locations.

The Nominated Officer shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

ONYX GLOBE PAYMENT LTD will use the Canadian Anti-Money Laundering Institute training programs and offered training sessions for regular updates of internal training programs (https://www.camli.org). Also ONYX GLOBE PAYMENT LTD will use others learning possibilities which are offered by well-known and reputable organisations (for example ACCP, ACAMS, ICA).

Role of the Employee

In the situation that an employee has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Transaction Report Form' (see appendix for example).

The STR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the Nominated Officer to discuss the reasons for their suspicion– however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below).

The timing for submitting the internal STR is important. The law states that an individual working in the regulated sector (i.e. EMI or API) should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company Nominated Officer.

Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options:

- Report the STR on to FINTRAC or RCMP or CSIS.
- File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to FINTRAC or RCMP or CSIS. The Nominated Officer should complete the Nominated Officer STR Resolution form in the event he decides not to make a report.

Frequently Asked Questions (FAQ)

Under what circumstances could I commit an Offence?

In the situation that an employee has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible.

An Offence may be committed:

- if employee does not follow KYC procedures accepted by Nominated Officer

- if flagrant violation of AML, KYC procedures are detected

What do you mean by 'Suspicion'?

Suspicion can occur in circumstances that suggest to a reasonable individual that a person might be laundering money or financing terrorism or financing proliferation or violate sanction regime. Suspicion must be more than a mere hunch. Any activity that does not fit with the normal course of business or is not normal for a particular client should be regarded as suspicious.

What do you mean by a Transaction?

A transaction is anything you carry out by way of business.

Suspicion indicators for new customers can include:

- Checking their identity is proving difficult;
- The customer is reluctant to provide details of his/her identity;
- There is no genuine reason for the customer to use the services of a merchant;
- Where transactions involve international transfers or foreign currency, the explanation for the business and the amount involved is unreasonable;

Suspicion indicators for regular and established customers include the:

- Transaction is different from the normal business of the customer;
- Size and frequency of the transaction is not consistent with the normal activities of the customer;
- Pattern of transactions has changed since the business relationship was established;

How do I report my suspicion to the Nominated Officer?

You should report the grounds for your suspicion to your Nominated Officer in line with your employer's internal procedures. You should include full details of the identification you have and any other customer information you have.

When should I report my knowledge or suspicion to the Nominated Officer?

You must do this as soon as is practicable after you have reasonable grounds for suspicion. If you do not do this, you may be committing an offence.

What does "as soon as is practicable" mean?

This means as soon as you reasonably can. Internal reporting lines to your Nominated Officer should be short in order to avoid delay.

What if I become suspicious before I complete the transaction?

You should make an internal report before the transaction is completed and wait for consent from your Nominated Officer before you complete the transaction.

What should I say to delay the transaction without "tipping off" the customer?

Give the customer an excuse that fits the circumstances. In difficult cases speak to your Nominated Officer or manager.

If I think delaying the transaction would "tip-off" the customer, can I go ahead?

Ask your Nominated Officer. They may let you proceed with the transaction, but this should not be done routinely. The reason why you think delaying the transaction would "tip off" the customer must be included in your report.

What should I do if the customer asks for his money back before I get consent from the Nominated Officer?

Seek advice from the Nominated Officer urgently.

What if I become suspicious after the transaction has taken place?

Make an internal report to your Nominated Officer as soon as you can.

What if I refuse the business?

If you refuse the business because you are suspicious, you must still make a disclosure to the Nominated Officer. You must obtain evidence and keep records of the customer's identification as soon as you become suspicious.

Identifying the Customer

'KYC' - What does 'know your customer' mean?

KYC means obtaining information about a customer over and above the required ID.

The ONYX GLOBE PAYMENT LTD has implemented a KYC program to ensure all kinds of customers (natural or legal persons or legal structures) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented throughout all ONYX GLOBE PAYMENT LTD divisions. The purpose of this is to reduce the risk of the ONYX GLOBE PAYMENT LTD being used for money laundering and financing of terrorism.

Multiple online directories of individual and business information are used to check all customer/client ID details before a full Individual or Business e-account is activated.

For Business clients we also check their details against the public business registers (for example BUSINESS REGISTERS OF THE PROVINCES AND TERRITORIES.

The following "Know Your Customer" procedures will be helpful in identifying prospective face-to-face or non-face-to-face customers who may present money-laundering and financing of terrorism and financing of proliferation risks. The ONYX GLOBE PAYMENT LTD applies a risk-based approach towards "know your customer" with reference to a customer's geographic ties, chosen products and / or services. A risk-based approach is applied as low, medium or high. This risk-based approach indicates the risk of whether the given customer may use or will use the ONYX GLOBE PAYMENT LTD services and/or products for financial crime.

In all cases, prior to taking on a new customer or engaging in a transaction with a customer with whom we do not have well-established relationship, the ONYX GLOBE PAYMENT LTD completes sufficient due diligence to have confidence in the integrity of the customers and the lawfulness of the proposed transaction by following actions:

1. Make reasonable efforts to determine the true identity of all customers and the legal and beneficial ownership of all accounts.

2. Determine the customer's citizenship, home and business addresses, occupation or type of business. Where appropriate, obtain supporting documentation.

3. Inquire whether the customer will have the sole interest in the account or whether there will be other persons who will have access to it. Verify the identity of all such persons and engage in any necessary due diligence regarding such other persons.

4. If the customer is not an individual;

a. Determine the legal status (e.g., corporation, partnership or other form of entity).

b. Determine whether the customer is regulated, either in the ONYX GLOBE PAYMENT LTD or a foreign country.

c. Determine all principal persons of the customer, such as officers and directors, or persons who have a substantial beneficial interest (i.e. own equal or more than 25% share in the company). As per the PCMLTFA Regulations, ONYX GLOBE PAYMENT LTD shall ensure that corporate and other legal

entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership. This includes details of beneficial interests held.

d. Obtain copies of all relevant organizational documents.

5. Identify the source of the customer's funds.

6. Screen the customer for:

a. Matches under the OFAC list;

b. Global Affairs Canadian sanctions list;

c. Account holders from countries listed on the Financial Action Task Force ("FATF"), NCCT list found the FinCEN advisory list;

d. Persons with significant holding, that hold over 25% equity or more in a business are now subject to AML/CTF screening;

e. sanctions match;

f. Visa Inc. and MasterCard Worldwide lists and Risk programs;

7. Where appropriate, obtain information regarding the frequency with which the customer expects to transfer funds to or from the account, i.e. monthly, quarterly, or the nature of any third-party payments to or from the account;

8. Where appropriate, obtain and contact reputable references, such as professionals and other members of the financial industry, banks, securities companies, etc.

9. Government Officials and Foreign Bank Accounts.

Special procedures apply for accounts for the benefit of politically exposed persons (PEPs), including senior government and political figures, particularly from certain countries, and for accounts opened by or through foreign banks and for clients from countries or industries deemed high risk. The ONYX GLOBE PAYMENT LTD performs enhanced due diligence and on-going due diligence measures proportionate with the risk of the customer. High risk customers will therefore be subject to enhanced due diligence and on-going due diligence. On-going due diligence processes will be applied to all existing customers within a specific period that will be determined by whether they are defined as high, medium or low.

In as much as this is not a regular part of the Company's business, you must consult the Compliance Officer before opening any account of this type.

10. Accounts through an Intermediary;

Where accounts come through an intermediary, the Agent must either perform due diligence with respect to the account or satisfy itself that the intermediary has performed the type of due diligence with respect to the account that would satisfy the Agent's "Know Your Customer" policy.

a. The scope of this due diligence will vary depending upon the Agents historical relationship with the intermediary, whether the intermediary is itself a regulated entity and the jurisdiction in which the intermediary is located. The Compliance Officer should be consulted as to the type of due diligence necessary for a specific intermediary.

b. At a minimum, due diligence of an intermediary should include a review of the intermediary's anti-money laundering and counter terrorism financing procedures. Where appropriate, representations from the intermediary as to its compliance with its procedures may be obtained.

c. Generally speaking, except for intermediaries who are regulated in an appropriate jurisdiction or are well-known by the Agent to have proper anti-money laundering and counter terrorism financing procedures in place, you should perform reference checks through published sources and others.

11. Counterparties;

The same rules set out in item 10 above also apply to transactions with counterparties on behalf of our customers. For this purpose, counterparties include private transaction counterparties and banks and other dealers, agents and intermediaries. While a relatively low level of due diligence will be required for counterparties who are regulated within a country known to have appropriate and well-enforced anti-money laundering and counter terrorism financing regulations, other counterparties will require the same level of due diligence as clients.

Business relationship establishing process

Individual E-Voucher

All individual E-Voucher holders would have to provide a certified photo ID and proof of residence (e.g. Utility bill) for their accounts to be activated and operational. E-Vocher holders should send a copy of their certified photo ID, i.e. International Passport, ID card, Driving License, Residence Permit, Visa Work Permit or other Verification ID and a copy of their proof of residence to ONYX GLOBE PAYMENT LTD depending on certain limits. The customer is also subjected to an AML/CTF/CPF sanctions screening.

Successful applicants will be notified via email or in personal cabinet that their E-Voucher has been upgraded to a Full functional.

Please note; If necessary, additional information may be requested by ONYX GLOBE PAYMENT LTD on the details regarding the nature of certain transactions.

All hard and soft copies of documentation from individual customers will be retained for a minimum of five years. All verified documents will be reviewed annually to ensure that they are: a) still relevant to the activity being carried out by the customer and b) are still valid (i.e. the ID documents provided have not expired).

Business e-Account

Merchant services

The Merchant services has been designed for businesses wishing to set up an account for corporate services. Before establishing business relationships, the potential customer must provide certain information details.

Details should include:

• A completed Application Form with signed T&Cs,

• Incorporation documents; certificate, Memorandum of Understanding and Articles of Association, company utility bill (proof of address);

• Details of ownership (those persons or entities which hold 25% or more shares), directors and personnel who will be operating on behalf of the business, including copy of passport and utility bill,

• Information regarding the nature of their business; including the amounts of money involved and the expected frequency of transactions. During this stage, the reason for using ONYX GLOBE PAYMENT LTD

services, the nature and level of the activity to be undertaken and the origin and destination of the funds should be clarified and noted.

• Any business related certification

• Any other relevant information regarding the business operations relating to use of our services/interface/platform,

• If necessary additional information may be requested by ONYX GLOBE PAYMENT LTD on the details regarding the nature of certain transactions.

If it is deemed necessary, please ask for all or selected Business KYC information to be certified as a true copy of the original by a solicitor.

This information should be emailed or sent to ONYX GLOBE PAYMENT LTD via post.

Successful applicants will be notified via email by ONYX GLOBE PAYMENT LTD employee on the need to sign a cooperation agreement.

All hard and soft copies of documentation from business clients will be retained for a minimum of five years. All verified documents should be reviewed annually to ensure that they are: a) still relevant to the activity being carried out by the business customer and b) are still valid (i.e. the company registered details and key company personnel details are still the same).

Keeping client information current

The PCMLTF Regulations require ONYX GLOBE PAYMENT LTD keep CDD and KYC information up to date. Regulations requires a ONYX GLOBE PAYMENT LTD to take reasonable steps to keep client identification information current. ONYX GLOBE PAYMENT LTD should update this information any time there is a material change in the client's circumstances. For this purposes ONYX GLOBE PAYMENT LTD provides on-going CDD for all clients with regularity depending on the clients level of risk.

Frequently Asked Questions (FAQ)

What is a business relationship?

A business relationship is one which:

- Helps in the carrying out of transactions on a frequent, habitual or regular basis and
- Where the total amount of any payment to be made is not known, or capable of being known, at the outset.

Just because your customer is a business does not mean you have a business relationship with them. A business relationship is when you treat a customer in a different way than the way in which you treat your one-off customers.

How will I know if the customer wishes to establish a business relationship?

You must ensure that you obtain sufficient information about the nature of any new business you deal with, including the amounts of money involved and the expected frequency of transactions. At the first transaction, you should establish the:

- Reason for establishing the business with you,
- Nature and level of the activity to be undertaken and
- Origin and destination of the funds.

You should also consider why the customer is using your services.

Why is evidence of identity important?

In order to follow the trail of laundered money, law enforcement authorities need to know the names of people involved.

When is identification required?

You must confirm and retain the ID of any customer who:

- Wishes to establish a business relationship with you involving frequent or regular transactions and the total value of transactions is not known at the start,

- As mentioned above CDD should be carried out not only on all new customers but also at appropriate times to existing customers on a risk sensitive basis, or when relevant customer change, or when the obliged entity has any legal duty.

- Conducts any transaction that you know or suspect might involve either the proceeds of crime or is to be put to criminal or terrorist use.

Do I need to check ID for small value transactions?

You are obliged to check ID for small value, or limited transactions unless it is within a business relationship - provided money laundering is not suspected.

From whom should I take evidence of identification?

Normally, you must take this evidence from your customer. In instances where your customer is or appears to be acting on behalf of someone else, you must obtain ID evidence from everyone in the chain.

What should I do when a customer wants to carry out a transaction that requires identification?

You should:

- Check evidence of ID at the first transaction,

- Where possible, retain a photocopy of the evidence or at the very least, record and retain information that would enable a copy to be obtained,

- Check it on a regular basis and satisfy yourself that the customer is who they claim to be.

What are the best forms of identification evidence?

The law states that you must satisfy yourself that the person is who they say they are. The identity document must have been issued by a federal, provincial, territorial or state government authority and must be valid (not expired).To be considered acceptable, the valid identity document must include:

- name
- date of birth
- photo
- signature.

Some combinations of identification are:

- passport (an international passport is acceptable if it includes the name, date of birth, photo and signature of the applicant and is accompanied by a professionally translated version if not in French or English)
- driver's license
- enhanced driver's license
- Canadian military identification card

- government-issued identification card
- government-issued enhanced identification card
- health card
- Canadian citizenship card (issued before February 1, 2012)
- Canadian permanent resident card
- U.S. permanent resident card (green card)

Please note, all identification evidence must include the individual photographs

What if I am still not satisfied?

Where you are presented with insufficient evidence, you may decide to make additional checks by, for example, phoning a third party after asking your customer to nominate someone to vouch for them. The telephone number of the third party must be listed in the telephone directory.

If you are still not entirely satisfied with the identification presented to you, you should refuse the business and report to your Nominated Officer, who will then decide whether to pass it on to FINTRAC or RCMP or CSIS .

What checks should I make on the document evidence given to me?

You should:

- Check the date of birth compared to the customer's appearance in the photo ID and
- Compare spellings of names and addresses on each document.

Please discuss any abnormalities found in the results with the Nominated Officer.

(see Annex: 4 for details on checks to be made)

What must I do when my customer is a company?

Where your customer or supplier is a limited company, you should identify the individuals who you deal with who have authority within that company to move funds, (not just cheque signatories) and obtain details of the company's:

- Registered number, corporate name and any trading names used,
- Registered address and any separate principal trading addresses,
- Photo ID,
- Profile check,
- Public business registers check to validate the name, address and directors of the company. If the client registered is not a director of that company, the ONYX GLOBE PAYMENT LTD will ask a director of that company to sign a company member additional user form. This will then give the person that has registered authorisation to use and operate on behalf of that company.

How often should I update my customer's record of ID?

You need only update the evidence of ID if something has changed. For example, you may need to update their address details if they move. It is advisable that information held is reviewed on an annual basis, to ensure that it is still up to date/valid.

(see Annex: 4 for more information)

Record Keeping

You will need to hold all records of business transactions for at least five years from the date that the business relationship ends.

Why do we have to keep records for five years from the end of a business relationship?

It's the law. The purpose of keeping records is to enable law enforcement to reconstruct business transactions; often well after the original business has been concluded. In making and retaining records you should have in mind the need to provide a clear audit trail of the business you have conducted.

The records that must be kept are:

- A copy of, or the references to, the evidence of the customer's identity obtained under the customer due diligence requirements as per the regulations
- The supporting records in respect of the business relationships or occasional transactions that are the subject of customer due diligence measures or on-going monitoring.
- Record of when the first client identification and verification took place, and how.
- Documents justifying exemption from identification, if applicable.

In relation to the evidence of a customer's identity, businesses must keep the following records:

- A copy of the identification documents accepted and verification evidence obtained, or
- References to the evidence of customer's identity.

Transaction and business relationship records (for example, account files, relevant business correspondence, daily log books, receipts, cheques, and so on) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect account or customer.

What is an audit trail?

An audit trail is a step by step record by which financial data can be traced to its source. In the case of money laundering the aim of establishing an audit trail is to trace the funds through to the first transaction (the placement) to identify the launderer.

What records do I have to keep?

The records that we keep must be sufficient enough to form a complete audit trail for customs officers to follow from the start of the transaction to the end; this is particularly important should the transaction later become part of an on-going investigation by law enforcement.

There are several different types of records we should keep:

- A copy of the evidence of identification presented. Photographic evidence is particularly valuable.
- Details of where the copies of identification can be found, which should be filed and easily recoverable. You must keep these records for at least five years from the date when the relationship with your customer finishes.
- Business records. You must keep a record of all transactions, regardless of whether the ID of the customer or client needed to be verified, for five years.
- All records of disclosures. Letters received from FINTRAC or any other correspondence with a law enforcement agency should be retained for at least five years.

Please note: We retain Individual customer and business client records for at least a five-year period after the business relationship has ended.

Identifying Suspicious Activity

Having identified a customer and conducted the necessary due diligence, we will be in a good position to spot anything unusual with the customers, their actions, inactions or transactions.

Look out for any suspicious actions or activity at every dealing stage with the customer. For example, this can be an unusual remittance abroad or a transaction amount that is not in normal line of activity.

The following list provides several types of behavior or activity that may be suspicious. The list is not exhaustive and not conclusive. Rather employees who have contact with customers, intermediaries or counterparties should use the list as a guide for inquiry and follow up:

- The customer wishes to engage in transactions that lack business sense or are inconsistent with the client's stated business/strategy.
- The customer exhibits unusual concern for secrecy, particularly with respect to his identity, type of business or dealings with companies.
- Upon request, the customer refuses to identify or fails to indicate a legitimate source for his funds.
- The customer exhibits an unusual lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to operate as an agent for an undisclosed principal but is reluctant to provide information regarding the principal.
- The customer has difficulty describing the nature of his business. The customer lacks general knowledge of his industry.
- For no apparent reason the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a haven for money laundering.
- The customer, or a person publicly or known to be associated with the customer, has a questionable background including prior criminal convictions.
- The customer account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- The customer account shows numerous currencies or cash transactions aggregating to significant sums. This is however not relevant as ONYX GLOBE PAYMENT LTD does not have any cash transactions.
- The customer account has a large number of wire transfers to unrelated third parties.
- The customer account has wire transfers to or from a bank-secrecy haven country or country identified as a money laundering risk.
- The customer account has unusual transactions or transactions that are disproportionate to the customer's known business.

Also, FINTRAC has issued the following guidelines on suspicious transactions with more specific ML/TF indicators related to MSB:

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer wants to pay transaction fees that exceed the posted fees.

- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Customer wants a cheque issued in the same currency to replace the one being cashed.
- Customer wants cash converted to a cheque and you are not normally involved in issuing cheques.
- Customer wants to exchange cash for numerous postal money orders in small amounts for numerous other parties.
- Customer enters into transactions with counter parties in locations that are unusual for the customer.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.
- Customer makes large purchases of traveller's cheques not consistent with known travel plans.
- Customer makes purchases of money orders in large volumes.
- Customer requests numerous cheques in small amounts and various names, which total the amount of the exchange.
- Customer requests that a cheque or money order be made out to the bearer.
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Customer purchases a large volume of money orders and changes payment type to avoid reporting requirements.

If you identify suspicious activity, contact the Nominated Officer who is responsible for issuing a Suspicious Transaction Report through the FINTRAC online system. The Nominated Officer should also notify senior management.

Note: DO NOT raise any concerns with the customer or use words to suggest you are not happy with anything that may tip them off.

Reporting Suspicions

Anti-money laundering processes require a team approach. Money laundering issues are complex. The Nominated Officer of ONYX GLOBE PAYMENT LTD should not attempt to shift through them alone and if the officer becomes aware of any suspicious circumstances, or have any questions, the officer should promptly consult with the Nominated Officer and Compliance Team of ONYX GLOBE PAYMENT LTD.

Suspicious Transaction reports – internal company process

In the situation that an employee (for this purpose, collectively, staff members) has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Transaction Report Form'.

The STR should contain as a minimum the following information:

- Details and identification data of all parties to the transaction
- The owner of the monies in question
- How the identity of the client was verified
- A full description of the transaction
- Reason for suspicion and supporting evidence

- Details of any assets which are subject to international sanctions

If in doubt, the staff member should call the Nominated Officer to discuss the reasons for their suspicion – however, they should be careful not to do this whilst the customer is standing in front of them or via any communication exchanged with the customer (they may 'tip off' the customer otherwise, see below).

The timing for submitting the internal STR is important. The law states that an individual working in the regulated sector should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

Where a staff member becomes aware that a customer wants to carry out a transaction which is suspicious and the timing for the transaction allows it, the staff member must ensure that 'consent' is given before processing the transaction. 'Consent' means that the company has sought and obtained approval from the FINTRAC to process the transaction. Further information on 'seeking consent' is provided below.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company Nominated Officer.

Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options:

Report the STR on to FINTRAC or RCMP or CSIS.

(see procedure below);

File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to FINTRAC or RCMP or CSIS;

The Nominated Officer should complete the Nominated Officer STR Resolution form (see appendix for sample) in the event he decides not to make a report to FINTRAC or RCMP or CSIS.

Making a Suspicious Transaction Report

In the situation that an employee has suspicions about a customer and/or transaction, he must ensure that the company Nominated Officer is notified about his suspicions as soon as possible.

Staff should use the internal 'Suspicious Transaction Report Form' (see appendix for example).

The STR should contain as a minimum the following information:

- Date/time of transaction
- Amount
- Customer name/customer ID information (e.g. passport number, etc)
- Transaction number
- Reason for suspicion of transaction

If in doubt, the staff member should call the Nominated Officer to discuss the reasons for their suspicion– however, they should be careful not to do this whilst the customer is standing in front of them (they may 'tip off' the customer otherwise, see below).

The timing for submitting the internal STR is important. The law states that an individual working in the regulated sector (i.e. MSB) should make a report as soon as he or she becomes suspicious. This may mean either before the transaction takes place or immediately afterwards.

However, staff may decide that there would be a danger that if they were to seek consent for a particular transaction (i.e. in advance of the transaction taking place) that there might be a danger that the customer would be 'tipped off'. See below for more information on 'tipping off'.

All staff members will have fully discharged their duties, and will have the full protection of the law, once a report of their suspicions has been made to the company Nominated Officer.

Once the Nominated Officer receives the internal STR from the staff member, the Nominated Officer has two options:

• Report the STR on to STR on to FINTRAC or RCMP or CSIS

• File an internal note indicating why, on the basis of review of the circumstances around the transaction, it is judged not necessary to make a report to STR on to FINTRAC or RCMP or CSIS.

The Nominated Officer should complete the Nominated Officer STR Resolution form in the event he decides not to make a report.

'Tipping Off'

Any staff member needs to make a judgement as to whether any delay to the transaction ('consent request') would have the effect of 'tipping off' the customer.

It is a criminal offence under section 333 of the Proceeds of Crime Act 2002, to do or say anything that might either 'tip off' another person that a disclosure has been made or in any way prejudice an investigation. This means that businesses must not tell a customer:

- that a transaction was/is being delayed because consent from FINTRAC or RCMP or CSIS has been requested;
- that details of their transactions or activities will be/have been reported to FINTRAC or RCMP or CSIS;
- that they are being investigated by law enforcement.

In situations where delaying a transaction may inadvertently lead to 'tipping off', it will make sense to process the transaction and then ensure that a STR is submitted to the Nominated Officer as soon as possible after. The staff member will have the protection of the law as soon as a STR has been submitted to the Nominated Officer.

If in doubt about whether to proceed with a transaction, the staff member should immediately contact the Nominated Officer for advice.

Documentation

Supporting documentation is a cornerstone of our anti-money laundering and counter terrorism financing procedures.

Unrecorded steps are soon forgotten. Records assist in tracking relevant information and in demonstrating that the company/individual has conducted our business responsibly and with integrity. All interviews, searches and activities undertaken to verify integrity of transactions and persons must be documented and stored for reference by ONYX GLOBE PAYMENT LTD, OFSI and FINTRAC if and when required.

All records must be kept for a minimum of five years after the business relationship with the customer ends.

Anti-Money Laundering for Merchants

Do Merchants need to comply with compliance regulations?

The Company obtains all information necessary to establish to its full satisfaction the identity of each new Merchant/ Legal entity and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected sales volumes.

When a Merchant account has been opened, but problems of verification arise in the service relationship which cannot be resolved, ONYX GLOBE PAYMENT LTD can close the account and transfer the money to the Merchant bank account. While the transfer of an opening balance from an account in the customer's name in another organization subject to the same KYC standard will be considered, ONYX GLOBE PAYMENT LTD follow its own KYC procedures. ONYX GLOBE PAYMENT LTD can consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

Naturally, Merchants have the right to move their business from one organization to another. However, if ONYX GLOBE PAYMENT LTD has any reason to believe that an applicant is being refused service facilities by another organisation, the Company is duty-bound to engage in enhanced due diligence procedures to the customer.

ONYX GLOBE PAYMENT LTD will not agree to open Merchant account or conduct on-going business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff.

Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

Prohibited businesses, industries

The company has set itself the prohibition of the list of goods and services (industry):

1. Banknotes sales;
2. Drugs and the use of a drug or drug-like substance;
3. Arms and ammunition;
4. Jewelry, precious metals;
5. Reinsurance and insurance services;

6. Cash services (such as current Treasury, currency exchange offices, money transfer agents or other service providers that offer money transfer facilities);

7. Currency trading intermediary services (for example, forex dealers), except in cases where the provider is licensed or provided legal opinion and is carried out in the service provider's supervision;

8. Binary Options;

9. Multi-level marketing (MLM);

10. Antiques and art trade;

11. Pharmacies and pharmaceutical activity, pharmaceutical, proprietary medicinal products and pharmaceutical trade;

12. The sale of tobacco products;

13. Illegal / piracy audio or video recordings;

14. Infringing goods (counterfeit goods);

15. Sexual services, Adult;

16. Financial pyramid;

17. Debt collection services;

18. Accept assets that are known or suspected to be the proceeds of criminal activity;

19. Enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organisation or member of such or listed on sanction lists;

20. Maintain anonymous accounts, accounts for shell banks or pay-through accounts.

Merchant On-Boarding

Process of on-Boarding Merchants is conducted in conjunction with the Acquirer bank, which will provide services to ONYX GLOBE PAYMENT LTD.

1. Pre-check

A specific Pre-Application form must be filled in the beginning of on-boarding process. Please find the Form in Annex 5.

Initial Merchant check will take not more than 2 business days. The Merchant webpage, contacts against OFAC, MasterCard and VISA risk programs will be checked, as well as considering the business model and checking it according to Internal Prohibited and Restricted Industries.

2. Documents for due diligence

After the pre-approval to process is given, an employee collects via e-mail and forward to the ONYX GLOBE PAYMENT LTD Compliance Team and Acquirer Bank the full documentation package:

- Company registration documents issued in the country where the merchant is incorporated (e.g. Certificate of Registration, Articles and Memorandum, Certificate of Registered Address, Certificate of Directors, etc)

- Documents stating the ownership rights of the ultimate beneficial owner (e.g. Shareholder Certificate, Share Transfer, eRegister, etc)

- Identification documents with the holder's signature (e.g. ID Card, Passport, Driving License, etc.)
- Documents stating the rights to represent a company (e.g. Power of Attorney, Articles, Minutes of Meeting etc.)
- Agreements with partners and suppliers, if applicable;
- License, if applicable;
- Financial statements;
- Processing history.

ONYX GLOBE PAYMENT LTD in conjunction with Acquirer Bank's Lawyers will verify the validity of documents and will list documents which should be notarized.

3. Agreement signing

Once the business is approved by ONYX GLOBE PAYMENT LTD and Acquirer Bank, ONYX GLOBE PAYMENT LTD employee prepares the agreement along with all terms and conditions.

ONYX GLOBE PAYMENT LTD signs the agreement and sends to Merchant or meets Merchant for signing it. This agreement is sent to the Acquirer bank as well.

All those documentation (i.e. agreement and application forms) merchant signs must be notarized or signed during onsite visit.

Annex 1: Risk Based Assessment

The object of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its Regulations is to detect and deter money laundering and terrorism financing. In 2008, the Government introduced amendments to the PCMLTFA and its Regulations to enhance the Canadian anti-money laundering and anti-terrorism financing (AML/ATF) regime. As part of these amendments, the Risk-Based Approach (RBA), which requires reporting entities to conduct assessments of their exposure to money laundering and terrorism financing risk using a number of prescribed criteria, was introduced.

Risk may be established both on the basis of objective criteria and subjective criteria. A 'risk rating' is given to each criterion.

Risk Ranking	Grading
L	Low-risk
M	Medium-risk
H	High-risk
PR	Prohibited

The Company, as part of its AML Program, has conducted 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 the Company to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment is routinely performed at the inception of a customer relationship, for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account. Thus, the monitoring of customer transactions and ongoing reviews is a fundamental component of the Company's risk based approach. In addition, this type of risk assessment process may also be adjusted for a particular customer based upon information received from a competent authority.

The Company 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 the Company 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 the Company's unique circumstances.

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 the Company because of the standing of the issuer and the nature of the measures;

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. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk;

Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them; or Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

The risk associated with countries and geographical areas, ONYX GLOBE PAYMENT LTD consider the risk related to:

a) the jurisdictions in which the customer and beneficial owner are based;

b) the jurisdictions that are the customer's and beneficial owner's main places of business; and

c) the jurisdictions to which the customer and beneficial owner have relevant personal links.

The company defines a list of jurisdictions with which it does not cooperate, as well as a list of high-risk countries based on FATF high-risk and other monitored jurisdictions, The Basel AML Index, Transparency International index, Canadian and U.S. sanctions programs etc.

ONYX GLOBE PAYMENT LTD does not handle transactions or onboard any customer from non-cooperation countries list.

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, the Company 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:

Customers conducting their business relationship or transactions in unusual circumstances, such as:

- Significant and unexplained geographic distance between the Company and the location of the customer;
- Frequent and unexplained movement of accounts to different institutions; and
- Frequent and unexplained movement of funds between institutions in various geographic locations.

The structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests of the customer.

Cash (and cash equivalent) intensive businesses including:

- 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);
- Casinos, betting and other gambling related activities; and
- Businesses that while not normally cash intensive generate substantial amounts of cash for certain transactions.

Charities and other "not for profit" organizations which are not subject to monitoring or supervision (especially those operating on a "cross border" basis).

"Gatekeepers" such as accountants, lawyers, or other professionals holding accounts at the Company, acting on behalf of their clients/cardholders, and when the Company places unreasonable reliance on the gatekeeper.

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

Customers that are Politically Exposed Persons (PEPs).

Product and Service Risk.

This category of risk includes the determination of potential risks presented products and services offered by the Company, such as risks associated with new or innovative products or services and the following factors:

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

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

Services involving banknote and precious metal trading and delivery; or

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.

Other Risk Variables.

The Company'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:

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.

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 the Company to treat the customer as lower risk.

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. Additionally, companies and their wholly owned subsidiaries that are publicly owned and traded on a recognized exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate and recognized regulatory scheme, which generally pose less risk due to the type of business they conduct and the wider governance regime to which they are

subject. Similarly, these entities may not be subject to as stringent account opening due diligence or transaction monitoring during the course of the relationship.

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.

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 the Company's own operations within the country.

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

Customer risk is also affected by Unusual Activity which may be suspicious:

- Split transactions – the customer is attempting to split a large transactions into several smaller transactions to avoid obligations to provide proof of source of funds
- New customers carrying out large transactions (as opposed to regular customers)
- Regular customer is processing transactions which do match the profile of previous transactions
- Customers processing transactions who do not appear to be legitimate owners of the funds (i.e. students processing large transactions)
- Customers involved in transactions which appear to be linked to transactions processed by other customers
- Customers who cannot provide ID when requested or who provide false ID
- Customers who cannot justify source of funds when requested
- Customer is not local to the business, (but not a tourist)
- Transactions where customer is accompanied or instructed by another person who tells him what to do

Risk Mitigation Strategies

The Company has implemented the following risk mitigation strategies:

1. Customer Identification, Due Diligence and Know Your Customer. The Company 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. In general, this program:
   1.1. Identifies and verifies the identity of each customer on a timely basis;
   1.2. Takes reasonable risk based measures to identify and verify the identity of any beneficial owner;
   1.3. Obtains appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions;
   1.4. 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:
      1.4.1.A standard level of due diligence that is applied to all customers when initiating or continuing a relationship, such as:
         1.4.1.1. Evaluating the nature of the relationship. As an example, determining the length of a customer's relationship with the Company, the products and services provided to a customer, and the manner in which a customer was referred to the

Company. The nature of a customer's relationship may serve to mitigate or to increase the overall risk indicators described below.

1.4.1.2. Identifying high risk geographies, including customers located in or conducting business transactions in High Risk Money Laundering and Related Financial Crime Areas; and

1.4.1.3. Identifying high risk entities, banking functions and transactions (refer to the High Risk Entities subtopic below).

1.4.2. The standard level being reduced in recognized lower risk scenarios, such as:

1.4.2.1. Publicly listed companies subject to regulatory disclosure requirements;

1.4.2.2. Other financial institutions (domestic or foreign) subject to an AML regime consistent with all AML recommendations;

1.4.2.3. 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

1.4.2.4. Transactions involving the minimum amounts for particular types of transactions (e.g. small insurance premiums).

1.4.3. 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 Company in relationships. These enhanced due diligence procedures include, but are not limited to:

1.4.3.1. Increased awareness by Company personnel of higher risk customers and transactions within business lines across the Company;

1.4.3.2. Increased levels of the Company's CIP, Know Your Customer (KYC), and enhanced due diligence;

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

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

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

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

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

2. Refer to the Customer Identification Program Policy and Know Your Customer Policy topics of this policy for detailed guidance.

2.1. Monitoring of Customers and Transactions. The degree and nature of monitoring performed by the Company is based upon its size, the AML risks that the Company 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.

2.2. 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 the Company's risk based monitoring system is to respond to enterprise wide issues based on the Company's analysis of its major risks. Monitoring under this risk based approach allows the Company 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. Refer to the appropriate topics of this policy for detailed guidance with respect to the monitoring of customers and transactions.

2.3. Suspicious Transaction Reporting. The regulatory and legal requirement to report suspicious transactions or activity by the Company 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 the Company. Therefore, a risk based approach for the reporting of suspicious activity under these circumstances is not applicable.

2.4. However, a risk based approach is appropriate for the purpose of identifying suspicious activity (such as directing additional resources at those areas the Company has identified as higher risk). In the same respect, the Company uses information provided by state and federal authorizes to enhance its approach for identifying suspicious activity. In addition, Management should always periodically assesses the adequacy of the Company's system employees training and assessment for identifying and reporting suspicious transactions.

2.5. Training and Awareness. The Company 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:

2.5.1. Tailored to the appropriate staff responsibility (e.g. customer contact or operations);

2.5.2. At the appropriate level of detail (e.g. front line personnel, complicated products or customer managed products);

2.5.3. At a frequency related to the risk level of the business line involved; and

2.5.4. Tested to assess knowledge commensurate with the detail of information provided.

Annex 2: Bribery Offences

DOMESTIC BRIBERY: LEGAL FRAMEWORK

Sections 121 to 123 of the Criminal Code prohibit the improper provision of benefits to Canadian government officials and employees. Section 426 of the Criminal Code criminalises private-sector bribery.

Offences involving bribery and corruption of Canadian government officials

Section 121(1)(a) of the Criminal Code prohibits the offering or giving of a benefit to a federal or provincial government official, or any member of his or her family, that creates a quid pro quo arrangement. An official that accepts such a benefit also commits an offence under this section. The purpose of this Section is to prevent exchanging benefits for influence in government and deter overt forms of domestic corruption.

Section 121(1)(b) prohibits giving a benefit to a federal or provincial government official in the course of business dealings between an accused and government. Section 121(1)(c) criminalises the receipt of such a benefit. The purpose of Sections 121(1)(b) and (c) is to preserve the appearance of integrity, rather than integrity itself. Unlike Section 121(1)(a), these offences do not require a quid pro quo arrangement. Also, written pre-approval from the head of the branch of government conducting business with an accused is a complete defence to Section 121(b) and (c) offences.

For the purpose of Sections 121(1)(a) through (c), government officials include employees or officials of: (1) federal and provincial governments; (2) government-controlled corporations; and (3) municipalities acting as agents of the federal or provincial crown.

Section 122 of the Criminal Code prohibits corruption of public officials in positions of trust. This Section criminalises using a public office for a purpose other than the public good if the misconduct arises to a serious and marked departure from the standard of responsibility and conduct expected of an individual in the accused's position of public trust. Under this section, public officials are not limited to federal or provincial government officials and include any person in a position of duty, trust, or authority, particularly if that person is in a corporation or the public service. Canadian courts have held that officials of First Nations bands are public officials for the purpose of Section 122.4

Section 123 of the Criminal Code functions the same way as Section 121(1)(a), but applies to municipal government officials.

What constitutes a benefit under the Criminal Code

Domestic bribery offences under the Criminal Code capture more than cash payments. Sections 121 and 123 of the Criminal Code each prohibit the payment or receipt of a 'loan, commission, reward, advantage, or benefit of any kind.' In R v. Hinchey, the Supreme Court defined a 'benefit' under the Criminal Code as anything that amounts to a 'material or tangible gain'. The Supreme Court also set out factors to determine whether something is a 'material or tangible gain', including the:

- relationship between the parties;
- history of reciprocal arrangements between the parties; and
- size or scope of the benefit.

Other Canadian courts have expanded these factors to include, in part, the:

- manner in which the gift was bestowed;
- nature of the provider's dealings with government; and
- state of mind of the provider and receiver.

Canadian courts have not identified a specific value threshold for what constitutes a benefit, but have identified specific items that do, or do not, constitute 'material or tangible gains'. Canadian courts have

found that hockey tickets,8 extravagant meals, gift cards over CAD 500, and payment for travel represent a material gain, but items such as infrequent and moderately priced meals, coffee, and low value promotional items do not.

Private corruption

Section 426 of the Criminal Code criminalises the provision or receipt of secret payments or benefits to or by an agent, including an employee, as consideration for actions related to the affairs or business of an agent's principal, including an employer. There are two separate offences contained in Section 426: (1) a donor offence, committed by a third party providing a benefit; and (2) an agent/recipient offence, committed by an agent receiving a benefit. These offences can be committed independently and do not require the donor and recipient to act in concert. Secrecy is a crucial element for this offence. There is no offence if an agent makes adequate and timely disclosure of the benefit to his or her principal.

Organisational liability

Pursuant to Section 22.2 of the Criminal Code, Canadian organisations can be party to offences committed by their 'senior officers' if the senior officer intended, in part, to benefit the organisation by committing the offence. An organisation can also be criminally liable if a senior officer:

- commits an offence themselves;
- directs other representatives of the organisation to commit an offence; or
- fails to take all reasonable steps to prevent another representative of the organisation from committing an offence the senior officer knew would be committed.

A 'senior officer' is defined broadly by the Criminal Code and includes any representative that plays an important role establishing an organisation's policies or manages an important aspect of the organisation's activities, including directors, chief executive officers, and chief financial officers. Canadian courts have found that even a general manager can be considered a 'senior officer' and create criminal liability for an organisation.

Liability of directors, officers, and employees

Under Section 21 of the Criminal Code, an organisation's directors, officers or employees may be charged as a party to an offence that the organisation itself has been charged with. A party to an offence under the Criminal Code includes anyone that commits an offence, or assists or encourages the commission of an offence. There is no strict or automatic liability for directors, officers or employees of organisations guilty of bribery. Instead, directors, officers or employees will only be guilty of a bribery offence committed by the organisation if they participated in or encouraged the commission of it.

Annex 3: Politically Exposed Persons Check

The definition of 'PEP' is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions
- Is an immediate family member of such a person
- Is a known associate of such a person
- Is resident outside or within the
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by –
- Any state;
- The European Community; or
- An international body; or
- Please note: An immediate family member or a known close associate of a person referred to in the paragraph immediately above does not necessarily qualify as a PEP without the appropriate risk assessment.

In cases where PEP is identified:

- Senior management approval should always be sought before establishing a business relationship with a PEP
- The source of funds should be established

The business relationship should be subject to enhanced and constant monitoring.

Establishing the source of funds

It is important that before a business relationship is entered into with a PEP their source of funds is established and Company is satisfied that there are no indications that funds that will be used for transactions to be carried out are derived from corruption (i.e. receipt of bribes), fraud or an attempt by the PEP to remove/hide assets from their home country.

The source of the PEP's funds may be established by asking the individual concerned a series of questions to determine from where they receive their money. These questions could include confirmation of the main source income (i.e. salary), any business interest or investments from which funds are/will be received.

Making a decision to transact with the PEP

In order to satisfy itself, below are areas on which questions can be asked of the PEP to determine whether a business relationship should be established- information from this can be presented to Senior Management of ONYX GLOBE PAYMENT LTD for them to make an informed decision:

- What is the position and the duties of the PEP- (please note that a less 'senior' PEP is less of a risk than heads of states, MP's, members of the Judiciary, Ambassadors)
- Are there any family members/close associates that are PEP's also?
- Identify the customer and the beneficial owner of the account.
- Know the customer's country of residence.
- Know the objective of opening the account and the volume and nature of the activity expected for the account.
- Obtain information on the occupation and the other income sources.
- Obtain information about the direct family members or associates who have the power to conduct transactions on the account.

Please note that currently ONYX GLOBE PAYMENT LTD is not transacting with any PEPs.

Annex 4: Internal Suspicious Transaction Report Format

SAR No: ...../.....

Particulars	Remarks
Date:	
ID of the customer:	
Name/address of Customer:	
Telephone no of Customer:	
Nature of suspicious activity:	
Give full detail of suspicion: [Include detail of transactions and identity checks.]	
Attach any relevant documents: 1. Transaction receipts 2. Proof of ID and Address 3. Sanctions list checks	
Name of the Reporting Officer:	
Signature by Reporting Officer:	
Refer to FINTRAC: [To be completed by Nominated Officer]	
Do not refer to FINTRAC: Reason for decision: Details	
Signature by Nominated Officer:	
Date referred to Nominated Officer Decision:	