Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

ANTI-MONEY LAUNDERING POLICY STATEMENT

It is the policy of XFORTA FINANCIAL TECHNOLOGIES LTD (the "Company") to comply with the "Money Laundering (Prevention) Act, 2011".

This policy statement is integral part of XFORTA FINANCIAL TECHNOLOGIES LTD's Anti-Money Laundering Policy, which includes procedures and personnel responsible for complying with this policy and applicable laws.

Reason for Policy/Purpose

The purpose of this policy is to ensure XFORTA FINANCIAL TECHNOLOGIES LTD's compliance with anti-money laundering laws and regulations, to assist law enforcement in combating illegal money laundering, and to minimize the risk of XFORTA FINANCIAL TECHNOLOGIES LTD's resources being used for improper purposes. Failure to comply with anti-money laundering regulations could result in civil and criminal penalties to XFORTA FINANCIAL TECHNOLOGIES LTD and/or individual employees and Directors.

Who Needs to Know This Policy

All XFORTA FINANCIAL TECHNOLOGIES LTD's Staff, Management and its Directors need to know this policy.

Policy/Procedures

Money laundering is the process of concealing the existence, illegal source, or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate. XFORTA FINANCIAL TECHNOLOGIES LTD is committed in assisting the Financial Intelligence Unit in detecting, preventing and eradicating terrorist financing and terrorist and criminal activity. XFORTA FINANCIAL TECHNOLOGIES LTD will evaluate all financial transactions and take all necessary steps to comply with anti-money laundering laws and regulations, listed in detailed in the Company's Policy and Procedure Manual.

Client Identification Procedures

As part of XFORTA FINANCIAL TECHNOLOGIES LTD's AML policy, the Company has established procedures to ensure that all clients' identities are verified prior to opening an account. Before opening an account for an individual client, XFORTA FINANCIAL TECHNOLOGIES LTD will require

satisfactory documentary evidence of a client's name, address, date of birth, and either but not limited to the following forms of identification:

1. Passport ID and number
2. Driver's License
3. Letter of Reference (one from a Company or financial institution and one professional/ business reference.
4. Cross check (World Compliance, Office of Foreign Assets Control, etc.)

For a corporation or other legal entity, XFORTA FINANCIAL TECHNOLOGIES LTD will require Satisfactory legal evidence of the entity's name, address and that the beneficiary and operators have been duly authorized to open the account. The AML Compliance Officer will retain records of all documentation that have been relied upon for client/corporation identification.

Prohibited Client

XFORTA FINANCIAL TECHNOLOGIES LTD will not open accounts or accept funds or securities from, or on behalf of, any person or entity nor accept high-risk clients (with respect to money laundering or terrorist financing) without conducting enhanced, well-documented due diligence regarding such prospective client.

Training and Review

The AML Compliance Officer will conduct Semi-annual employee training programs for all personnel regarding the AML policy. Such training programs will review applicable laws, regulations and recent trends in money laundering and their relation to XFORTA FINANCIAL TECHNOLOGIES LTD's business. Attendance at these programs is mandatory for all personnel, and session and attendance records will be retained for a three-year period.

Who Approved This Policy

Board of Directors - XFORTA FINANCIAL TECHNOLOGIES LTD.

INTRODUCTION

The prevention of money laundering in Canada is governed by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17). This document is available to all staff. Staff is required to review the information contained in these documents as well as these internal guidelines at least quarterly. The Company's internal guidelines also adopt the best international standards including the anti- money laundering objectives of Section 313 (a) and 319 (b) of the US

Patriot Act of 2001 without incorporating foreign laws into the overall Banking regimes of Canada or into XFORTA FINANCIAL TECHNOLOGIES LTD.

These anti-money laundering provisions are designed to meet international standards and have been adopted and approved by the Board of Directors at a Board meeting held January 11th, 2021 and shall be updated and enforced through the executive management committee comprising representatives of the Board along with the Company's President, Chief Operating Officer and Chief Compliance Officer, who shall report directly to the Company's Chief Operating Officer and Chairman on all compliance issues Section 2(1) of the Canada Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) defines "money laundering" as:д

- Engaging, directly or indirectly in a transaction that involves property that is the proceeds of crime, knowing or having reasonable grounds for believing the same to be proceeds of crime.
- Receiving, possessing, managing, investing, concealing, disguising, disposing of or brining into Canada any property that is the proceeds of crime, knowing or having reasonable grounds for believing the same to be the proceeds of crime.

Money Laundering is punishable by a fine of between twenty-five thousand to one hundred thousand dollars and/or imprisonment for a term of between three and five (5) years.

Attempts are sometimes made to use the Banking system for the purpose of money laundering. Most such attempts involve either inducement or deception of Company staff to accept deposits or the transfer of funds, securities and other negotiable instruments, which are the proceeds of crime, or to provide safe custody facilities for such funds or assets.

The most common form of Money Laundering encountered on a day-to-day basis takes the form of accumulated cash transactions deposited in the Banking system or exchanged for value items. Electronic fund transfer systems increase the vulnerability of the Banking system by enabling the cash deposits to be switched rapidly between accounts in different names and between different jurisdictions.

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) creates specific procedures and standards that, when adhered to, will ensure that our Company, and the Canada Banking system at large, remains free of tainted funds and other assets. The Act requires

that we maintain a business transaction record. This record includes, where relevant, the following:

1. The identification of all the persons party to that transaction - Review Activity Report
2. A description of that transaction sufficient to identify its purpose and method of execution
3. The details of any account used for the transaction, including Company, branch and sort code
4. The total value of that transaction.

It is the Company's policy to ascertain the above information as required by law and to effectively maintain client records for a period of not less than five years from the termination of the Company / customer relationship. A financial institution commits a criminal offence if it fails to keep a financial transaction record as required by the Act.

The Director of the Financial Service Unit may, on reasonable suspicion, that a money laundering offence is being committed or has been or is about to be committed, enter or authorize someone to enter into the premises of any financial institution during normal business hours to inspect the institution's financial transaction record and ask any questions relevant to such record and to make any notes or take any copies of the whole or any part of such record. The Act also requires that financial institutions pay special attention to all complex, unusual or large business transactions, or unusual patterns of transactions whether completed or not, and to all unusual patterns of transactions and to insignificant but periodic transactions, which have no apparent economic or lawful purpose.

Management must review the Large Transactions Report from the DDA Module and all incoming and outgoing wire transfers. It is a criminal offence for a financial institution to fail to report or to report falsely such suspicion. It is also a criminal offence to inform or "tip off' the person or institution which is the subject of the report or investigation.

BEARING IN MIND THE REQUIREMENTS IMPOSED ON US BY THIS LAW AND OTHER RELEVANT LAWS, OUR POLICY IS:

To conduct all necessary due diligence procedures in order to ascertain the true identity of all the Company's customers, or potential customers. In this way we will ensure that assets are not invested in our Company anonymously or under assumed or fictitious identities;

To provide for enhanced due diligence on any client deemed to be a "politically exposed person" (PEP); a client engaged in a high risk business such as Internet commerce, or money services

businesses; a client engaged in business in any jurisdiction in which there is active military conflict, suspicion of large scale drug production or terrorist activity; and/or a recurring high dollar volume of business activity or unexpectedly large "one-off" business transactions. In addition to the Company's standard account opening and monitoring procedures, when a client or transaction falls into an "enhanced due diligence" category, the specific transaction(s) must be reviewed by the Company's Chief Compliance Officer for determination as to whether a suspicious transaction report shall be filed with the Canada FINTRAC's Financial Intelligence and the Financial Intelligence Unit (FIU);

To take steps to verify that all assets deposited into the Company are from legitimate sources so as to ensure that assets that are the proceeds of crime are not deposited in or otherwise invested in our Company;

To ensure that Company personnel comply with the need to maintain the financial transactions record required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17);

To ensure that Company personnel are properly trained to maintain vigilance regarding all unusual transactions or series of transactions. Where there is reasonable suspicion that any such transaction or series of transactions constitute money laundering, to forthwith report such suspicions on Form STR to the FINTRAC's Financial Intelligence, as required by law;

To comply fully with the guidelines and training requirements promulgated by the FINTRAC's Financial Intelligence in an effort to maintain Canada's good reputation as an ethical financial center committed to combating economic crimes;

To define and confirm with the established rules of good conduct in Company management;

To ensure that the Company maintains a comprehensive client information system that establishes the proper identification of both individual and institutional customers, as well as a thorough description of business activity and source of wealth/funds;

In addition to the establishment of initial KYC documentation when the client account is opened, the client shall be cross checked against OFAC "watch lists" not less than once annually with clients falling into the "enhanced due diligence" category being subject to being cross checked against the OFAC list not less than quarterly. To the extent practical, the Company shall engage Company software able to cross check clients against the OFAC lists automatically;

KYC documentation shall also include a client profile to allow the Company to understand typical and expected transaction types and levels for all clients. Unexpected transactions shall automatically trigger scrutiny of the Compliance Officer in undertaking enhanced due diligence on the transaction;

To have the Company AML policies and procedures reviewed by an independent outside auditor not less frequently than once a year as well as to be constantly prepared for periodic scheduled and unscheduled audits by the FINTRAC's Financial Intelligence and the FIU;

These guidelines constitute the official policy of the Company. They will remain in force until amended by the Board of Directors in compliance with legislation or subsidiary legislation enacted by the Government or FINTRAC's Financial Intelligence. They are, however, subject to the following conditions:

5. Except where specifically provided by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17), or other relevant law, the Company's obligation to maintain the confidentiality of its customers continues.
6. It is not the intention of these guidelines to:

Incorporate foreign currency, fiscal or other economic regulations into our law and thereby make them to be applicable to our Company (unless this is already the case under existing international treaties and the law of Canada); Affect the current legal and fiduciary relationship that has traditionally existed between Company and its customers (save as if necessary to comply with the requirements of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) or other relevant laws).

7. These guidelines set out standard rules for avoiding money laundering activities in the conduct of the Company's business and are iii accordance with the code of professional ethics; they are not intended to impede the efficient provision of normal services for bona fide clients.
8. These guidelines are intended to ensure the accurate determination of a customer's identity and to permit thereby the efficient accomplishment of the Company's obligation to maintain an adequate financial transactions record and testify and furnish information, as provided for by Canada law. All customer records must be held for a minimum of five (5) years.

9. These guidelines are intended to ensure that the Company operates with international "best practices" for combating the spread of money laundering while respecting the legitimate confidentiality needs of our clients and the privacy laws of Canada.

PROHIBITED ACTS

Company personnel shall be prohibited from performing the following acts:

- The opening and maintaining of accounts without having ascertained the identity of (the beneficial owner of the account).
- The provision of any other services to a customer without having first observed the due prudence amid diligence necessary to ascertain the assets or funds are from a legitimate source.
- The Company will not provide correspondent accounts to foreign shell companies or companies which refuse to provide a certification that they are not operating as a foreign shell Company.
- The Company will not provide services to companies or individuals offering Internet casinos or other forms of on-line gambling.
- The Company will not provide information on its clients to third parties except as stated herein or by compulsion of law.

OBSERVANCE OF CARE IN ACCEPTING FUND

ASCERTAINING THE IDENTITY OF THE BENEFICIAL OWNER

The Company will not open payment accounts, unless it has ascertained with such care as is reasonably possible in the circumstances the identity of the person beneficially entitled to the funds to be credited or to be invested;

I. SCOPE OF APPLICATION

The staff's obligation is to verify the identity of the prospective customer before opening of accounts, irrespective of whether such accounts are maintained under the name of an individual or a corporation.

In the case of cash equivalent transactions (exchange, purchase and sale of precious metals, cash subscriptions to Company issued medium term notes and bonds, etc.), the obligation of staff is to check the identity of the contracting party and verify the source of funds in any transaction which exceeds US $10,000 or equivalent).

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

II. IDENTIFICATION OF THE CONTRACTING PARTY

A. Individuals

The Company checks the identity of the contracting party having no fixed domicile or being domiciled abroad by means of an official identity document (i.e. passport, identity cards, driving license, etc).

B. Legal entities and companies

- The identity of legal entities is to be examined by obtaining confirmation of the address indicated by the entity by way of postal delivery or some other equally valid method;
- Identity checking of such a contracting party is to be effected by way of an extract from a commercial register or from some other equally reliable document (e.g. memorandum, articles and certificate of incorporation).

All account signatories for a company must be duly accredited. In the case of a of an account for clubs, societies, and charities, the Company will satisfy itself as to the legitimate purpose of the organization by, for example, requesting a copy of the constitution. Where there is more than one signatory to the account, the identity of at least two signatories should be verified initially and, when signatories change, care will be taken to ensure that the identity of at least two current signatories have been verified.

III. ASCERTAINING THE IDENTITY OF THE BENEFICIAL OWNER

The identity of the beneficial owner of the assets to be deposited is to be ascertained at the time of opening the account or deposit.

All reasonable care must be exercised in identifying the beneficial owner. The Company may assume that the contracting party and the beneficial owner are identical. This can no longer be assumed, however, if unusual circumstances are brought to the attention of the Company;

A. Legal entities and companies

If the contracting party acts for the account of a legal entity or company, the Company shall register the entity's name, address and country of domicile.

IV. CASES OF DOUBT

If any doubts arise, the procedure set out below shall be implemented.

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

V. SURVELLIANCE

The Company has to ensure that its internal control department and its auditing firm can check as to the indication procedure being carried out.

Verify clients' background via World Compliance and The US Department of Treasury - Office of Foreign Assets Control (OFAC) databases.

Appropriate records are to be kept of the name, registered name, address and country of domicile of the contracting party as well as of the means used to establish identity. Any documents obtained in the case of legal entities are to be preserved; The details as to the identity of the beneficial owner of the individuals controlling the company must also be preserved.

PROCEDURES IN CASES OF DOUBT

In cases of doubt, when opening accounts or deposits, the Company shall require a written declaration from the customer as to whether he is acting for his own account or for the account of a third party and in the latter case, for whose account. For example, doubt is justified in the following cases:

The opening of an account or deposit is requested, and, at the same time, a power of attorney is going to a person not recognizable as being closely enough related to the account holder (e.g., to a foreigner), or if any other unusual aspects arise;

The opening of an account or a deposit is requested by a person whose financial situation is known to the Company. The assets handed over or to be remitted are beyond the limits of the customer's recognized financial ability;

The opening of an account or a deposit is requested by a person domiciled abroad, who has been introduced to the Company. At the same time, a power of attorney is given to a person who is recognized as not being in a sufficiently close relationship to the account holder

The opening of an account or a deposit is requested by a person domiciled abroad, who has been introduced to the Company and whose financial situation is known to the Company. The assets, handed over to be remitted are beyond his final situation;

The opening of an account or a deposit is requested by a person domiciled abroad who has not been recommended to the Company. The discussion the Company must have with the customer at the time of opening the account or deposit brings to light unusual aspects; The opening of an account or a deposit is requested by a person domiciled abroad by way of correspondence,

accompanied by an attestation of the signature but the potential customer is not personally known to the Company.

Where serious doubt remains as to the accuracy of the customer's written declaration, which cannot be eliminated by further clarification, the Company must decline the request for the opening of the account or deposit.

VI. STR – SUSPICIOUS TRANSACTION REPORT

It is the policy of the Company to report all suspicions of Money Laundering transactions to the supervisory authority which has been designated by law as the Financial Intelligence Unit. (No 35 of 2002 Part IV, Section 20) It is further the Company's policy to file suspicious transaction reports with the FIU on all complex, unusual or large business transactions, unusual patterns of transactions (whether completed or not) and insignificant but periodic transaction that have no apparent economic or lawful purpose. The Company may also consider the following indicators in determining whether a STR report should be filed:

- Does the client appear to be living beyond his or her means?
- Is the client's business activity inconsistent with sales (i.e. unusual payments from unlikely sources), industry averages or financial rations?
- Does the client have a history of changing bookkeepers or accountants yearly?
- Is the client unable to locate and provide company records?
- Is the client's company consistently in a loss position but continued to exist without a reasonable explanation of the continued loss?
- Does the company have shareholder loans not consistent with business activity?
- Does the company make large payments to subsidiaries or similarly – controlled companies that are not within the normal course of business?
- Is the company invoiced repeatedly and does it make transactions to organizations located in countries that do not have adequate money laundering laws?
- Does the client make statements about involvement in criminal activity?
- Is the client continually accompanied by and watched by third parties?
- Does the client show uncommon curiosity about internal systems, controls, policies or have unusual knowledge about laws relating to suspicious transaction reporting or anti-money laundering laws?

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

- Does client attempt to convince an employee not to complete documentation required for the transaction?
- Does the client present confusing details about a transaction or try to over justify or explain the transaction?
- Does the client seem secretive or nervous about the transaction?
- Has the client's home or business telephone been disconnected shortly after an account was opened.
- Does the client use aliases and/or a variety of similar but different addresses?
- Does the client offer Company employees money, gratuities or unusual favors for the provisions of services that may appear unusual or suspicious?
- Does the client provide doubtful or vague information?
- Does the client produce seemingly false identification or identification that appears to be counterfeit, altered or inaccurate?
- Does the client refuse to produce personal identification documents?
- Does the client attempt to establish identity using something other than his or her personal identification documents or does he attempt to open accounts in a false name?
- Does the client's supporting documentation lack important details such as a telephone number or are they impossible to check for some other reason?
- Does the identification documents presented appear brand new?
- Does the client transaction seem inconsistent or fail to have any economic purpose?
- Does significant activity suddenly appear on an inactive or dormant account?
- Does the transaction involve a country where illicit drug production or exporting may be prevalent or where there is no effective anti-money laundering system?
- Does the transaction involve a country known to or suspected to facilitate money laundering activities? bb) Does the client offer multimillion dollar deposits from "confidential sources"?
- Does the client have transactions involving an offshore "shell" Company whose name may be similar to the name of a major legitimate institution?
- The obligations of Financial Institutions and its internal reporting procedures require that proper records be kept for use in compiling an audit trail during money laundering investigations and prosecutions.

These records are to include customer identification and related transactions. Specifically showing the identity of any or all customers as well as particulars for each transaction carried out for each customer.

These records are to be kept in a secure environment for a period of at least five years after the institution has carried out the last relevant financial business. The objective is to allow authorities to retrieve relevant available information without undue delay. If there is an ongoing investigation when the five-year limit occurs, the records should be kept until the authorities have closed the case.

The customer identification records should clearly show the type of evidence of identification obtained from the customer and specifically show sufficient details of the customer's identity. A copy of this evidence must be kept as a part of the customer's record.

The transaction records must be admissible in court proceedings and are to include all related information necessary to carry out the transactions. These refer to any records or information that leads to entries into the accounts of the financial institution or the customer's specific account. For example, properly prepared cheques, telegraphic transfers, credit/debit slips, etc. In the case of wire transfers, all information related to senders and beneficiaries should be included in the payment messages.

In maintaining the customer identification records and the transaction records - keep in mind that they may be used to develop an audit trial. They should include enough information to allow authorities to locate:

- the beneficial owner of an account
- the amount of money going into and out of an account
- the origin of money
- the form in which money was deposited and withdrawn
- the destination of money
- the identity of the person performing the transaction

the form of instruction for the transaction.

EDUCATION AND TRAINING GUIDE IN MONEY LAUNDERING PREVENTION AS PER STATUTORY REQUIREMENTS

The purpose of this guide is twofold:

The Financial Institution must adopt appropriate measures to keep abreast of policies and procedures as governed by law regarding the prevention of money laundering in an effort to protect its interests.

The Financial Institution must ensure that staff be familiar with current policies and procedures in place to prevent any possibilities of money laundering occurrence. In so doing, staff must be reminded of the responsibility of their role within the organization. The guide is classified into three main categories:

- Establish an effective "Know Your Customer" policy.
- Establish a detailed record keeping of deposits/withdrawals and procedures of transactions.
- Establish a log for the handling of suspicious transactions.

I. "KNOW YOUR CUSTOMER POLICY"

The Company will never establish a relationship with a customer until it knows the customer's true identity. If a potential customer is unwilling to provide the necessary information, the relationship should be reconsidered. If the Company has established a customer relationship, it should be alert for any unusual business transactions. The Company has, therefore, provided formats, which adequately cover all criteria required for the establishment of such a relationship. At the onset of interviewing a customer, should there be a reluctance to provide information as set in our Banking requirements; the proper thing to do is to obtain Management's decision as the ultimate decision. A caution note can be discretely put in this customer's file for future referral. Pointers For a Personal Account:

- Identification of owner of account — preferably Passport with photo or Drivers license with photo.
- Occupation of person and type of business.
- Complete home and business address.
- At least two references showing evidence of a satisfactory Banking relationship with an acceptable financial institution for a minimum of two years, signed by a senior official for easy referrals.
- If possible, query how customer was referred to us.
- Verify clients' background via World Compliance and The US Department of Treasury - Office of Foreign Assets Control (OFAC) databases. Pointers For a Joint Account

- Requirements are the same as “Pointers for a Personal Account” above.

Pointers for a company account

Requirements are the same as the above and the following:

- If Company is not incorporated in Canada, notarized copy of Certificate of Incorporation, Copy of Articles of Association and Memorandum of Association.
- List and signatures of Directors of the Company (these are included in formats provided by the Company.
- Two Company references on all Directors and authorized signatures.
- Evidence that the Company is in good standing for at least one-year

II. DETAILED RECORD KEEPING OF DEPOSITS/WITHDRAWALS AND PROCEDURES OF TRANSACTIONS

A customer file is to be immediately established in which all personal or company data will be lodged. Along with this, copy of the complete transaction including copies of entries is to be kept for at least five years. In respect to cheques deposited, a copy of this item will be lodged for referral. No funds will be released. Funds will be “frozen” for the appropriate period until clearance as stipulated in the Company’s manual. In respect to wire transfers, a copy of incoming/outgoing telex will be placed on file. Information such as Company source, sender’s name, reference number, transaction date, and dollar amount is to be logged. At a minimum, we should have on hand information on:

- The origin of funds.
- The form in which funds were deposited or withdrawn.
- The identity of the person who conducted the transaction and his/her signature on record.
- His/her signature on record.
- The destination of the funds. The form of instruction or authority.

Customers that walk in with large dollar amounts must present evidence of declaration of funds brought into the country either at the International Airport, the borders, or at the FINTRAC’s Financial Intelligence. The Company must retain this form duly stamped by a Government Body to protect its interests. This form will or should show where the source of funds originated. Our Source of Funds form must be completed. In addition, the following lists of internal reports routinely produced are of major support:

- Large Transaction Deposits/Withdrawals Report
- Suspected Kiting Report
- Incoming and Outgoing Wire Transfer Logs
- Monetary Log for items $3,000 and above.

III. SUSPICIOUS TRANSACTIONS

While it is difficult to define what is a suspicious transaction, a simple hint would be when in doubt, query. Look out for anything out of the ordinary on the basis of "know your customer." It is therefore, recommended that staff familiarize themselves with customer's activities in order to recognize when a transaction is unusual. Bear in mind, however, an unusual transaction may not necessarily be a suspicious transaction. Some helpful hints are:

- Beware of activity not consistent with the customer's business.
- Beware of attempts to avoid reporting or record keeper requirements.
- Be conscious of funds transfer activities.
- Beware of a customer providing false information.

Again, any of the above may not be illicit activity; it only means that the transaction may require closer scrutiny. Nevertheless, as a precautionary measure, should a situation arise, it should be properly documented or authorized by senior management for reporting purposes. It is the Company's objective to provide refresher training at regular intervals in an effort to:

- Detect suspicious activity in a timely manner.
- Comply with all regulatory laws.
- Promote safe and sound practices
- Minimize the risk that the Company will be used for illicit activities.
- Protect the Company's reputation.

Staff sessions to discuss these issues are to be encouraged in order to get feedback coupled with added training support provided by the FINTRAC's Financial Intelligence.

IV. MONEY LAUNDERING – STAGES OF THE PROCESS

Placement

This is the first stage in the washing cycle. Money Laundering is a "cash-intensive" business, generating vast amounts of cash from illegal activities (for example: street dealing of drugs where payment takes the form of cash in small denominations). The monies placed into the financial

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

system or retail economy or are smuggled out of the country. The aims of the launderer are to remove the cash from the location of acquisition so as to avoid detection from the authorities and to then transform it into other assets forms, (for example: travelers checks, postal orders, etc.).

Layering

In the course of layering, there is the first attempt at concealment of disguise of the source of the ownership of the funds by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. The purpose of layering is to disassociate the illegal monies from the source of the crime by purposely creating a complex web of financial transactions aimed at concealing any audit trail as well as the source and ownership of funds.

Typically, layers are created by moving monies in and out of the offshore Company accounts of bearer share shell companies through electronic funds transfers. Given that there are over 500,000 wire transfers – representing in excess of $1 trillion – electronic circling the globe daily, most of which is legitimate, there is not enough information disclosed on any single wire transfer to know how clean or dirty the money is, therefore providing an excellent way for launderers to move their dirty money. Other forms used by launderers are complex dealings with stock, commodity, and future brokers. Given the sheer volume of the daily transactions, and the high degree of anonymity available, the chances of transactions being traced is insignificant.

Integration

The final stage in the process. It is this stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the “cleaned” money into the economy is accomplished by the launderer making it appear to have been legally earned. By this stage, it is exceedingly difficult to distinguish legal and illegal wealth. Methods popular to money launderers at this stage of the game are:

- The establishment of anonymous companies in countries where the right to secrecy is guaranteed. They are then able to grant themselves loans out of the laundered money in the course of future legal transactions. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.
- The sending of false export-import invoices overvaluing goods allows the launderer to move money from one company and country to another with the invoices serving to verify the origin of the monies placed with financial institutions.

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

- A simpler method is to transfer the money via wire-transfer to a legitimate Company from a Company owned by the launderers, as “off the shelf Companies” are easily purchased in many tax havens.

V. MONEY LAUNDERING – MONEY LAUNDERING METHODS

How the basic steps mentioned in the Stages Of The Process are used depends on the available laundering mechanism and the requirements of the criminal organizations. The table below provides some typical examples. Placement Stage Layering Stage Integration Stage Cash paid into Company (sometimes with staff complicity or mixed with proceeds of legitimate business). Wire transfers abroad (often using shell companies or funds disguised as proceed of legitimate business). False loan repayments or forged invoices used as cover for laundered money. Cash exported Cash deposited in overseas Banking system. Complex web of transfers (both domestic and international) makes tracing original source of funds virtually impossible. Resale of good/assets. Cash used to buy high value goods, property or business assets. Income from property or legitimate business assets appears “clean”.

These are a small selection of the ways that people clean their “dirty money”. These schemes are still being used on unsuspecting businesses as even though the authorities know about them, not many people do, or even have access to this type of information.

ESTABLISH AN EFFECTIVE “KNOW YOUR CUSTOMER” POLICY

Firm “Know Your Customer” policies are a Company’s most effective weapon against being used unwittingly to launder money. Knowing customers, including depositors and other users of Company services, requiring appropriate identification, and being alert to unusual or suspicious transactions can help deter and detect laundering schemes.

A “KNOW YOUR CUSTOMER” POLICY TAILORED TO THE COMPANY’S OPERATIONS:

Helps detect suspicious activity in a timely manner; Promotes compliance with all Banking laws; Promotes safe and sound Banking practices; Minimizes the risk that the Company will be used for illicit activities; Reduces the risk of Government seizure and forfeiture of a customer’s loan collateral when the customer is involved in criminal activity, and Protect the Company’s reputation.

Generally, a Company should never establish a relationship with a customer until it knows the customer’s true identity. If a potential customer is unwilling to provide the necessary information,

the relationship should be reconsidered. If the Company has established a customer relationship, it should be alert for any unusual business transactions. What We Should Look For

The following situations may indicate money laundering. These lists are not all-inclusive, but can help us recognize ways launderers may approach them.

- Beware of Activity not Consistent with the Customer's Business
- Beware of Unusual Characteristics or Activities
- Beware of Attempts to Avoid Reporting or Record-keeping Requirements
- Beware of Certain Funds Transfer Activities
- Beware of a Customer who Provides Insufficient or Suspicious Information
- Beware of Certain Company Employees, and
- Beware of Changes in Company Transactions.

Transactions like those mentioned above may warrant attention. Just because a transaction appears on the list does not mean that it involves illicit activity. It only means that the transaction requires close scrutiny. Many of these activities are suspicious only because they are inconsistent with the normal customer behavior. Such transaction may upon closer examination be found to be legitimate business activity. Similarly, other transactions note mentioned may be suspicious if they are inconsistent with the normal activity of a particular customer.

Two important aspects of knowing your customer are:

10. Being satisfied that a prospective customer is who he claims to be and is the ultimate client; and
11. Ensuring that sufficient information is obtained on the nature of the business that the customer expects to undertake, as well as any expected or predictable pattern of transactions. This information is updated as appropriate and as opportunities arise.

1. As part of the due diligence process, a XFORTA FINANCIAL TECHNOLOGIES LTD:

- Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset1 of a business relationship. This process should include, where appropriate:
    a. Taking reasonable measures to understand the ownership and control structure of the customer;

b. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and

c. Discontinuing the transaction, if customer documentation information is not forthcoming at the outset of the relationship.

- Employ enhanced due diligence procedures for high risk customers or transactions or business relationships such as private Banking operations, non-resident customers, trust arrangements, companies having nominee shareholders or customers who the Company has reasons to believe are being refused Banking facilities by another Company;
- Monitor account activity throughout the life of the business relationship; and
- Review the existing records if there is a material change in how the account is operated or if there are doubts about previously obtained customer identification data.

2. In effecting the due diligence process, XFORTA FINANCIAL TECHNOLOGIES LTD:

- Whenever possible, require prospective customers to be interviewed in person. Exceptions to this are outlined in the sections on Non-face-to-face Customers and Introduced Business;
- Use official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to opening the account or establishing the business relationship (whether permanent or occasional or whether natural person or legal arrangements). Identification documents which do not bear a photograph or signature and which are easily obtainable (e.g. birth certificate and driver's license) are not acceptable as the sole means of identification. Verification may involve the use of external electronic databases.
- In instances where original documents are not available, only accept copies that are certified by an approved person (see Appendix 6). Approved persons should print their name clearly, indicate their position or capacity together with a contact address and phone number;
- If the documents are unfamiliar, take additional measures to verify that they are genuine e.g. contacting the relevant authorities.

3. For the purpose of these Guidelines, XFORTA FINANCIAL TECHNOLOGIES LTD will seek to identify the customer and all those who exercise control over the account/transaction. A customer includes:

- A person or entity that maintains an account with XFORTA FINANCIAL TECHNOLOGIES LTD

- A person or entity on whose behalf an account is maintained i.e. beneficial owner;
- The beneficiaries of transactions conducted by professional intermediaries such as lawyers, accountants, notaries, business introducers or any other professional service providers; or
- Any person or entity connected with a financial transaction that can pose a significant risk to XFORTA FINANCIAL TECHNOLOGIES LTD, including persons establishing business relations, purporting to act on behalf of a customer or conducting transactions such as: Opening of deposit accounts; Entering into fiduciary transactions; Renting safety-deposit boxes; Requesting safe custody facilities; and Occasional transactions exceeding thresholds as discussed below or linked transactions under this benchmark, and all occasional wire transfers.

4. Generally, XFORTA FINANCIAL TECHNOLOGIES LTD should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, verification of customer identity and beneficial owner may be undertaken following the establishment of the business relationship provided that:

- It is done as soon as reasonably practicable;
- It would be essential not to interrupt the normal conduct of business (e.g. non face-to-face business and securities transactions);
- The money laundering risks are effectively managed. Should XFORTA FINANCIAL TECHNOLOGIES LTD determine this to be an unacceptable risk, we will retain control of any funds received until verification requirements have been met. If the requirements are not met and XFORTA FINANCIAL TECHNOLOGIES LTD determines that the circumstances give rise to suspicion, it should make a report to the FIU.

5. Where a customer is permitted to utilize the business relationship prior to verification, financial institutions should adopt risk management procedures under which this may occur. These procedures should include a set of measures on the limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions outside of the expected norm for the type of relationship.

6. Where the financial institution is unable to satisfactorily complete CDD requirements, it should not open the account, commence business relations or perform the transaction. It should also consider making a suspicious transaction report.

7. Where there is a suspicion that an asset is suspected to either stem from a criminal activity, or is linked or related to, or is to be used to finance terrorism or a transaction relates to money laundering or the financing of terrorism, XFORTA FINANCIAL TECHNOLOGIES LTD should be cognizant of the possibility of tipping-off a customer when conducting due diligence. XFORTA FINANCIAL TECHNOLOGIES LTD should make a business decision whether to open the account or execute the transaction as the case may be, but an STR should be submitted to the FIU.

ANTI-MONEY LAUNDERING IMPROVEMENT PROCESS

XFORTA FINANCIAL TECHNOLOGIES LTD's(XFORTA FINANCIAL TECHNOLOGIES LTD's) Compliance Officer under the supervision of its COO is to understand the relationship between individuals responsible for monitoring AML and Company management. XFORTA FINANCIAL TECHNOLOGIES LTD's Compliance Officer or its COO is to ensure that the individuals responsible for monitoring AML do not have sufficient authority (real and perceived) and influence in XFORTA FINANCIAL TECHNOLOGIES LTD (XFORTA FINANCIAL TECHNOLOGIES LTD).

Perform management's AML risk assessment of all major business lines, products, and services.

Compliance Officer under the supervision of its COO will conduct annual assessment and administered by our Compliance Officer. XFORTA FINANCIAL TECHNOLOGIES LTD will look at risk as a product of volume, regulation, staff turnover, regulator focus. XFORTA FINANCIAL TECHNOLOGIES LTD will also look at more than simply cash transactions, we will also analyzed each of the Company's lines of business to determine how it might be abused by money launderers.

Provide copy of most recent Board approved AML policy and procedures.

Compliance Officer under the supervision of its COO will maintain records of when the Board of Directors last reviews XFORTA FINANCIAL TECHNOLOGIES LTD's policy and procedures. The Board

of Directors supports the XFORTA FINANCIAL TECHNOLOGIES LTD's AML efforts and is committed to provide the staffing and other assets needed to implement this policy. XFORTA FINANCIAL TECHNOLOGIES LTD will ensure the AML policy reflects the current regulatory environment and are review annually.

Properly maintain the most recent Board approved Know Your Customer Policy (KYC).

Compliance Officer, under the supervision of its COO will update any future changes and assure that the policy is being followed by our staff, by providing semi-annual training. XFORTA FINANCIAL TECHNOLOGIES LTD will engage FINTRAC's Financial Intelligence for any current updates in regards to AML and will make the necessary updates in the XFORTA FINANCIAL TECHNOLOGIES LTD Policy and Procedure Manual.

Properly maintain of policy and procedures relating to Suspicious Activity Report (SAR) reporting and monitoring requirements.

Compliance Officer under the supervision of its COO will review how XFORTA FINANCIAL TECHNOLOGIES LTD handles SAR responsibilities. Ensuring all departments understand their roles in forwarding suspicions for centralized consideration and filing. Share lessons learned in documents, particularly those about reporting illegal or suspect actions that may affect the Company.

Review the most recent independent audit results regarding compliance, including management's responses.

Compliance Officer under the supervision of its COO will reviewed the most recent audit to determine whether, in our opinion, our Company is obtaining a thorough job.

XFORTA FINANCIAL TECHNOLOGIES LTD will properly maintain AML records of training schedule with dates, attendees, and topics.

Records will be maintained by the Compliance Officer or COO. Meetings at which these topics are discussed will be documented as part of these records. Ensure and determine whether there are employees who require initial or additional training.

Training files (for example, materials used for training.)

Compliance Officer under the supervision of its COO will include information that has been distributed to inform Company employees of AML requirements.

Xforta Financial Technologies LTD
info@fortapayments.com
319 W Hastings street, #400
Vancouver BC V6B 1H6
Canada

File of Suspicious Activity Reports (SAR)

Compliance Officer under the supervision of its COO will maintain in a file with any follow-up SARs, and of all of the reports or other documents used in the Company's research of the activity described in the reports. In addition, XFORTA FINANCIAL TECHNOLOGIES LTD should also maintain a file of any activity that the Company investigated and on which the Company determined not to file a SAR, including the rationale behind that decision.

Logs or other method reflecting incoming and outgoing wire transfers.

Compliance Officer under the supervision of its COO will analyze and determine whether such patterns of large wires-in followed by wires-out from a same client are justified based on the business or customer involved. Also analyze the types and volume of wire transfer activities conducted by the Company. Include methods of payment accepted for such transfers and also acceptable remitters (for example, accountholders versus non-accountholders).