Anti-money Laundering Policy For Know your Client

Policy Statement

CanaCash Financial Services Ltd. (the "Company") policy is to ensure proper adherence to the provisions and intent of the FINTRAC (the "Act") regarding the requirement to implement reasonable procedures to deter money laundering activities and actively search for suspicious activity. The AML Officer is responsible for reviewing any such activity and determining whether a Suspicious Activity Report (SAR) should be filed.

As such, it is the authority, basis and platform for the development, communication, implementation, interpretation and enforcement of appropriate and applicable operating procedures that follow in this section.

In general, the Company's Anti-Money Laundering Program (AML Program) is a risk based process that is imbedded within the internal controls of the Company. It is the responsibility of the Board of Directors and Senior Management to ensure that the Company maintains this effective internal control structure, including suspicious activity monitoring and reporting. The Company's AML Program is based upon the:

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

Changes to this policy require approval by the Board of Directors, Partners, owners (known hereafter as "Managers") of the Company.

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

The "Managers" have the authority to approve this policy, and annually approves the merit thereafter. Management is responsible for ensuring the directives are implemented and administered in compliance with the approved policy.

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

The primary responsibility for enforcement of this policy and its operating procedures rests with the "Managers" and our employees.

Definitions

Money Laundering. An activity criminalized by law.

1. Terrorist. An act of domestic terrorism or international terrorism.
2. Account. A formal business relationship established to provide regular services, dealings and other financial transactions, and includes, but is not limited to, a demand deposit or other transaction or asset account and a credit account.
3. Transaction. A credit or group of credits and their associated debits.

Structure of Accountability

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

   Specifically, the "Managers" are responsible for:

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

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

   Specifically, the AML Officer is responsible for:

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

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

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

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

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

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

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

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

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

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

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

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

K. Training Company personnel on AML Program directives; and

L. Supporting an independent AML audit program

3. Compliance Committee. The Compliance Committee to provide assistance to and support the AML Officer to promote effective management of the Company's AML Program

Specifically, the Board of Directors is responsible for:

A. Assisting the AML Officer in ensuring the compliance mandate established by this policy is an integral part of Company operations;

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

C. Providing guidance to the AML Officer to ensure the Company adapts to changes mandated by the law.

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

D. Reviewing and approving the Company's AML Program training program;

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

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

Risk Analysis and Assessment

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.

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

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

   In addition to Canadian Financial Action Organizations other sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units,

as well as relevant national government bodies and non-governmental organizations. 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;

C. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them; or

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

1. Customer Risk. Determining the potential money laundering or terrorist financing risks (to the extent that such terrorist financing risk can be identified) posed by a customer or category of customers is a critical component. Based on its own criteria, 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:

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

      i. Significant and unexplained geographic distance between the Company and the location of the customer;

      ii. Frequent and unexplained movement of accounts to different institutions; and

      iii. Frequent and unexplained movement of funds between institutions in various geographic locations.

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

   C. Cash (and cash equivalent) intensive businesses including:

      i. Money services businesses (e.g. remittance houses, currency exchange houses, money transfer agents and bank note traders or other businesses offering money transfer facilities or services);

      ii. Casinos, betting and other gambling related activities; and

      iii. Businesses that while not normally cash intensive generate substantial amounts of cash for certain transactions.

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

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

unreasonable reliance on the gatekeeper.

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

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

2. 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:

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

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

ii. International private banking services

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

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

3. Other Risk Variables. 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:

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

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

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

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

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

F. Use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that unnecessarily 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.

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:

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

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

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

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

      1. A standard level of due diligence that is applied to all customers when initiating or continuing a relationship, such as:

         i. Evaluating the nature of the relationship. As an example, determining the length of a customer's relationship with 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.

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

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

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

   i. Publicly listed companies subject to regulatory disclosure requirements;

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

   iii. Individuals whose main source of funds is derived from salary, pension, social benefits from an identified and appropriate source and where transactions are commensurate with the funds; or

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

3. The standard level being increased with respect to customers that are determined to be of higher risk due to the nature of their activities which may require increased monitoring.

   This may be the result of the customer's business activity, ownership structure, anticipated or actual volume or types of transactions, including those transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as correspondent Companying relationships and PEPs. These enhanced due diligence procedures include, but are not limited to:

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

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

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

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

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

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

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

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

2. 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.

3. 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.

4. 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.

5. 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.

   Refer to the Suspicious Activity Reporting topic of this policy for detailed guidance.

6. 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:

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

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

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

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

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

Refer to the Staff Training topic of this policy for detailed guidance.

Money Laundering and Terrorist Financing Red Flags

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

1. Customers Who Provide Insufficient or Suspicious Information.

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

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

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

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

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

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

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

H. A customer is a trust, shell company, or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

Company accounts for those shell companies while shielding the owner's identity.

2. Efforts to Avoid Reporting or Recordkeeping Requirements.

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

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

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

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

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

3. Funds Transfers

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

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

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

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

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

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

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

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

   I. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the

transfers, particularly when this activity involves high risk locations.

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

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

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

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

4. Electronic Funds Transfer

A. Large value, automated clearing house (EFT) transactions are frequently initiated through third party service providers (TPSP) by originators that are not Company customers and for which the Company has no or insufficient due diligence.

B. TPSPs have a history of violating EFT network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.

C. Multiple layers of TPSPs that appear to be unnecessarily involved in transactions.

D. Unusually high level of transactions initiated over the Internet or by telephone.

5. Activity Inconsistent with the Customer's Business

A. The currency transaction patterns of a business show a sudden change inconsistent with normal activities.

B. Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals

C. Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high risk countries (e.g., countries designated by national authorities as non-cooperative countries and territories).

D. The stated occupation of the customer is not commensurate with the type or level of activity

E. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self employed).

F. With respect to nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction

6. Employees

   A. Employee exhibits a lavish lifestyle that cannot be supported by his or her salary. TPSPs have a history of violating EFT network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.

   B. Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.

   C. Employee is reluctant to take a vacation.

Detection and Monitoring Procedures

The Company follows these policies and procedures that are implemented for the detection and prevention of money laundering activities as part of the Company's AML Program:

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

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

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

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

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

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

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

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

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

9. Monitoring business accounts by identifying the following activities:

   A. One or more cash deposits a week, which are structured, avoid CTR reporting. (Note: a payment to a card account is considered structured if it is between $8,000 and $10,000);
   B. Two or more instances a week, where a customer makes two or more cash deposits on the same day, and the total of the deposits is between $5,000 and $8,000;
   C. One or more instances a week, where a customer has made cash deposits to two or more related accounts, and the total of the deposits to a card account or multiply accounts is between $5,000 and $10,000;
   D. Cash deposits that are over $10,000, and, that are 25% greater than the customer's second highest cash deposit; (not applicable if over card limit)
   E. Cash deposits that are over $10,000, and, that are 150% of the customer's average cash deposits (ignoring inconsequential deposits that are below $3,000);
   F. Cash withdrawals of more than $5,000, unless the withdrawal is made for payroll purposes;
   G. Deposits of more than $3,000, made in traveler's checks or money orders;
   H. Purchase with cash of cashier's checks, travelers checks, or money orders for $3,000 or more.

Company procedures for compliance are as follows:

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

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

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

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

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

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

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

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

4. Designated Contact Person. The AML Officer is the point of contact for the Company for such investigative issues or similar requests for information from FINTRAC.

5. Use of Security Information. It is against Company policy to use information provided by FINTRAC in an investigation for any purpose other than:

   A. Reporting to FINTRAC;

   B. Determining whether to establish or maintain an account, or to engage in a transaction; or

   C. Assisting the Company in complying with this requirement.

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

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

6. No Other Action. It is against Company policy to take any action, or to decline to take any action, with respect to an account established for, or a transaction engaged in with, an

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

individual, entity, or organization named in a request from FINTRAC, or to decline to establish an account for, or to engage in a transaction with, any such individual, entity, or organization. Except as otherwise provided in an information request, such a request shall not require the Company to report on future account opening activity or transactions or to treat a suspect list received as described by the regulation

Information Sharing with Other Financial Institutions

The Company, under the protection of the safe harbor from liability, may voluntarily receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering.

The following rules apply:

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

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

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

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

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC

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

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

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

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

   The Compliance Officer for this policy is Cory McGinness. The responsibility of the Compliance Officer is to ascertain that Company policy is in compliance with the current laws and regulations, and that the policy is communicated to the appropriate employees and agents.

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

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

   Management approved this policy on January 2010

On behalf of the Board

For more information:

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

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

FINTRAC (Financial Transaction and Reports Analysis Centre of Canada) is responsible for investigation of money laundering and terrorist financing cases that are originating or destined for Canada. The financial intelligence unit was created by the amendment of the Proceeds of Crime (Money Laundering) Act in December 2001 (via Bill C-25) and created the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.Financial institutions in Canada are required to track large cash transactions (daily total greater than CAD$10,000.00 or equivalent value in other currencies) that can be used to finance terrorist activities in and beyond Canada's borders and report them to FINTRAC