GP WEALTH MANAGEMENT

INDEPENDENT THINKING WORKING FOR YOU

Anti Money Laundering & Terrorist Financing Policy & Procedures Manual

Date Created: June 13, 2008
Date Revised: August 2, 2011

Table of Contents

1.0 Introduction

The Anti Money Laundering & Terrorist Financing Manual provides for policies and procedures, which have been approved by senior management, documents the internal controls and procedures that must be adhered to by all Financial Advisors, Employees, Supervisors and Senior Management to ensure compliance with the Rules, By-laws and Policies of the MFDA and applicable securities legislation including detecting and deterring money laundering and financing of terrorist and criminal activity.

This manual is made available to all Financial Advisors, Employees, Supervisors and Senior Management and is maintained and updated regularly at head office. The most up to date version can be obtained on line by visiting the secured site at http://gpwealth.ca and clinking through to the "Dealer Services" section.

2.0 Overview of Money Laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. Profit-motivated crimes span a variety of illegal activities from drug trafficking and smuggling to fraud, extortion and corruption. While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

1. Placement: involves placing the proceeds of crime in the financial system;
2. Layering: involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds (e.g., the buying and selling of stocks, mutual funds, commodities or property); and,
3. Integration: involves placing the laundered proceeds back in the economy under a veil of legitimacy.

While GP Wealth Management Corporation ("GPWM") is most vulnerable at the layering stage of the process every effort must be made to prohibit and actively pursue the prevention of money laundering, terrorist financing and any activity that facilitates money laundering, terrorist financing or criminal activities. GPWM requires its officers, directors, employees, financial advisors and financial advisor staff to adhere to the standards set in this policy in preventing the use of products and services for money laundering, terrorist financing or other criminal purposes.

2.1 Compliance with AML and Terrorist Financing

GPWM supervisory staff is responsible to ensuring compliance with Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act and for initiating Suspicious Transaction Reports or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by such agencies related to the policy shall be directed to GPWM Compliance Department.

The duties for day to day operations are the responsibility of the GPWM Compliance Department. The responsibilities of GPWM supervisory staff with respect to the policy include, but are not limited to:

(a) the design and implementation of the policy;
(b) updating the policy as required;
(c) dissemination of information to officers, employees, financial advisors and financial advisor staff;
(d) providing training;

(e) monitoring compliance;
(f) maintaining necessary and appropriate records;
(g) reporting, when warranted; and
(h) Independently test the operation against the policy.

2.2 Covered Products

GPWM supervisory staff must adhere to the procedures for reviewing all products approved for distribution.

2.3 Account Holder Identification

2.3.1 Registered Accounts

It is not required to identify any individuals authorized to give instructions when opening a registered plan. Such plans include but not limited to:

(a) a registered retirement savings plan;
(b) a locked-in retirement plan;
(c) a group registered retirement savings plan;
(d) a profit sharing plan or a deferred profit sharing plan as long as the account is funded by the account-holder's employer

2.3.2 Additional General Exceptions to Account Holder Identification

If GPWM has confirmed the identity of an individual account holder, there is no need to confirm the account holder's identity again so long as the financial advisor recognizes the individual and the identification information is on file. If GPWM supervisory staff has any doubts about the identification information previously collected, it must identify the individual account holder again.

Once GPWM supervisory staff has confirmed the existence of a corporation (or other entity), confirmed its name, address and the names of its directors, it is not required to confirm the same information in the future PROVIDED THERE IS NO CHANGE IN THE INFORMATION.

2.3.3 Non-Registered Accounts

Identification of all individuals authorized to give instructions on a non-registered plan (account), including an entity account, must be ascertained before any transaction is carried out.
GPWM shall not approve a New Account Application for a Canadian resident client without either a Social Insurance Number ("SIN") or Business Identification Number ("BIN").

2.4 Transactions Involving Cash and Cash Equivalents

All account holder dealings involving cash, traveler's cheques, and bearer bonds are strictly prohibited. GPWM may accept cash equivalents such as bank drafts and money orders.

2.5 Electronic Funds Transfers

GPWM may accept electronic funds transfer-ins, through its banking institution, solely for the purposes of purchasing a financial product. GPWM shall not directly transfer-out funds.

2.6 Record Keeping

GPWM is responsible for keeping account opening records (account applications) and supporting documents. Additionally, GPWM must maintain the following records or ensure ready accessibility to them:

(a) Account-related records created in the normal course of business;
(b) Account holder statements that GPWM sends to the account holder;
(c) Suspicious transaction report record.

In addition, GPWM supervisory staff is responsible to ensure that the records are maintained properly and that Suspicious Transaction Reports are filed as required. All records must be maintained for a period of 7 years after the account holder plan is closed for any reason.

2.7 Risk Based Approach

GPWM uses a risk-based approach to assess potential threats and vulnerabilities to money laundering and terrorist financing. The approach encompasses at least the following:

(a) Risk assessment
(b) Risk mitigation
(c) Account holder identification and beneficial ownership information
(d) Ongoing monitoring of transactions

A Politically Exposed Foreign Person (PEFP) is an individual or a family member (mother, father, child, spouse/common law partner, spouse/common law partner's mother, father, brother, sister, half-brother, half-sister) of an individual who holds or has ever held one of the following offices or positions in or on behalf of a foreign country:

(a) a head of state or government;
(b) a member of the executive council of the government or member of a legislature;
(c) a deputy minister or equivalent;
(d) an ambassador or an ambassador's attaché or counsellor;
(e) a military general or higher rank;
(f) a president of a state owned company or bank;
(g) a head of a government agency;
(h) a judge;
(i) a leader or president of a political party in a legislature.

GPWM supervisory staff must determine whether an existing potentially high risk account holder and/or a new account holder is a PEFP. When there is a change in marital status or occupation for an existing account holder, GPWM supervisory staff must verify determine whether an existing account holder is a PEFP.

2.8 Checking the Office of the Superintendent of Financial Institutions Canada (OSFI) List

On a monthly basis, GPWM supervisory staff will compare its account holder database with the Office of the Superintendent of Financial Institutions Canada's Terrorism Financing List of Names. In the event of a match, GPWM supervisory staff must conduct further investigation of the account holder's

identification and circumstances, and bring the issue to the attention of the GPWM Compliance Department if the match is not a false positive.

Upon notification to the GPWM Compliance Department of a match to the OSFI list or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not limited to, a review of all available information such as account holder history, account history, birth dates and addresses.

2.9 Monitoring and Reporting

All suspicious transactions or attempted suspicious transactions must be reported immediately to Chief Compliance Officer or Compliance Department. If signs of suspicious activity based on certain indicators are determined, then a formal investigation will be performed before proceeding with the transaction.

If the results of the formal investigation warrant, a report will be filed with Financial Transactions Reports Analysis Centre of Canada (FINTRAC) and/or appropriate law enforcement and/or regulatory agency. Investigation results must not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall an officer, employee, financial advisor or financial advisor staff disclose or discuss any anti money laundering and terrorist financing concern, investigation, notice or Suspicious Transactions Report filing with the person(s) subject to such investigation. No action shall be taken against a person for making a report in good faith. All reports must be documented and retained.

2.10 Training

All individuals who conduct business on behalf of GPWM must be provided with training in anti-money laundering and terrorist financing prior to engaging in any business activity and after a material change in this policy. All such individuals must be provided a copy of this policy. The training will include at a minimum:

- how to identify suspicious transactions and attempted transactions using indicators;
- roles of the officers, employees, financial advisors, financial advisor staff and how to perform such duties and responsibilities;
- actions to take once a suspicious or attempted suspicious activity is detected;
- account holder identification;
- record retention;
- consequences for non-compliance with the policy.

Training is provided through presentations, conference calls, and compliance memos covering all of this policy. All training is documented to include the training date, names of persons trained, and mode and location of training.

The GPWM Compliance Department will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. In addition, the GPWM Compliance Department will maintain evidence of all training delivered.

2.11 Consequences for Non-Compliance

Money laundering facilitates corruption and can destabilize the economies of susceptible countries. There are significant consequences for GPWM officers, directors, employees, financial advisors and financial advisor staff for failing to comply with Canada's legislative requirements, such as:

FAILURE TO	CONSEQUENCES UPON CONVICTION
report a suspicious transaction or to make a terrorist property report	Up to 5 years imprisonment, up to a fine of $2,000,000 or both
report a large electronic funds transfer	A fine of $500,000 for a first offence and $1,000,000 for each subsequent offence
retain records	Up to 5 years imprisonment, up to a fine of $500,000 or both
Implement a compliance regime	Up to 5 years imprisonment, up to a fine of $500,000 or both
Implement any required element of the compliance regime	Monetary penalty of up to $100,000 for each element
report the required information, by an entity, to senior management within 30 days after the review of its compliance program	Monetary penalty of up to $100,000

3.0 Ascertaining Account Holder Identification

3.1 Obtaining the Identity of an Individual

A Financial Advisor must complete a GP New Account Application Form (NAAF) for each new plan opened for an account holder, and provide all the required information and supporting documentation.

GPWM and its supervisory staff will not approve a new account until the following is received at head office for review:

(a) a completed New Account Application Forms signed by the account holder and Financial Advisor
(b) all supporting documents are attached to the NAAF
(c) identification (if required) is attached to the NAAF

3.1.1 An Individual Physically Present

A Financial Advisor can identify an individual, who is physically present, by referring to the valid original of any two of the following documents:

1. Driver's License;
2. Passport;
3. Record of Landing;
4. Permanent Resident Card;
5. Birth Certificate;
6. Old Age Security Card;
7. Certificate of Indian Status;
8. Citizenship Card;
9. Social Insurance Number Card;
10. Health card issued by:

(a) British Columbia
(b) Alberta
(c) Saskatchewan
(d) Québec (only if the account holder offers to use it);
(e) New Brunswick
(f) Nova Scotia
(g) Newfoundland & Labrador

11. Provincial or territorial identification card issued by any of the following or their successors:

(a) the Insurance Corporation of British Columbia;
(b) Alberta Registries;
(c) Saskatchewan Government Insurance;
(d) the Department of Service Nova Scotia and Municipal Relations;
(e) the Department of Transportation and Public Works of the Province of Prince Edward Island;
(f) Service New Brunswick;
(g) the Department of Government Services and Lands of the Province of Newfoundland and Labrador;
(h) the Department of Transportation of the Northwest Territories;
(i) the Department of Community Government and Transportation of the Territory of Nunavut;

12. Foreign identification, if equivalent to an acceptable type of Canadian identification document.

The document must be valid at the time of ascertaining the account holder identity, must have a unique identifier number and it must have been issued by a federal, provincial or territorial government.
If an account holder wants to use a document other than listed above, consult GPWM's Chief Compliance Officer or Compliance Department regarding acceptability of the document and provide reason(s) behind the account holder's failure to provide any of the above documents.

3.1.2 An Individual Not Physically Present

Identify an individual, who is NOT PHYSICALLY PRESENT, by using a COMBINATION OF ANY TWO of the following three methods:

Method 1: Identification Product or Credit File Method

Refer to EITHER:

(a) an independent and reliable identification product. It must be based on personal information and Canadian credit history about the account holder of at least six months duration. This type of product can use a series of specific questions, based on the account holder's credit file, to enable verification of account holder identity; or
(b) the account holder's credit file with the account holder's permission. The credit file must have been in existence for at least six months

Method 2: Attestation Method

Obtain an attestation that an original identification document for the individual has been seen by a commissioner of oaths or a guarantor. The attestation must be on a legible photocopy of the document and include the following information:

(a) the name, profession and address of the commissioner of oaths or the guarantor;
(b) the signature of the commissioner of oaths or the guarantor;
(c) the type and number of the identifying document provided by the individual being identified.

In this context, the guarantor must be an individual engaged in one of the following professions in Canada:

(a) a dentist, a medical doctor or a chiropractor;
(b) a judge, a magistrate or a lawyer;
(c) a notary (in Québec) or a notary public;
(d) an optometrist or a pharmacist;
(e) an accredited public accountant (APA), a chartered accountant (CA), a certified general accountant (CGA), a certified management accountant (CMA), a public accountant (PA) or a registered public accountant (RPA);
(f) a professional engineer (P.Eng., in a province other than Québec) or engineer (Eng. in Québec);
(g) a veterinarian

Method 3: Cleared Cheque or Deposit Account Method

Confirm that EITHER:

(a) a cheque drawn on a deposit account that the account holder has with a financial entity has cleared; or
(b) that the account holder has a deposit account with a financial entity.

The cheque provided by the account holder must have the name of the account holder printed on it. A cheque with a handwritten name is unacceptable. The financial entity in this context must be a bank listed in Schedule I or II of the Bank Act, an authorized foreign bank with respect to operations in Canada, a credit union, a caisse populaire, a trust and loan company or an agent of the Crown that accepts deposit liabilities. The deposit account must be in Canada and must not be exempt from identification requirements for the financial entity, such as RRSP or reverse mortgage.

In each of the two methods used, the account holder’s information must be consistent:

(a) from one method to the other
(b) with other documents provided and;
(c) with information in GPWM records, if any.

If stricter requirements are imposed by an external business partner, then such requirements must be adhered to.

3.1.3 Unacceptable ID

1. Photocopies of acceptable ID's listed in section 3.1.1 above;
2. A birth or baptismal certificate issued by a church,
3. An identification card issued by an employer for its employee or a student card issued by a school, because these documents are not issued by a federal, provincial or territorial government;
4. An individual's provincial health card from Ontario, Manitoba or Prince Edward Island;
5. Void cheque to setup Pre-Authorized Contributions (PACs).

3.2 Obtaining the Identity for an Entity

A Financial Advisor must complete a GP New Account Application Form (NAAF) for each new plan opened for an Entity (account holder), and provide all the required information and supporting documentation.

GPWM and its supervisory staff will not approve a new account until the following is received at head office for review:

(a) a completed New Account Application Forms signed by the account holder and Financial Advisor
(b) all supporting documents are attached to the NAAF
(c) identification (if required) is attached to the NAAF

3.2.1 Corporations

For a corporate account, confirm the existence of the corporation, and its name and address by referring to:

1. certificate of incorporation; or
2. articles of incorporation; or
3. a record that has to be filed annually under provincial securities legislation; or
4. any other record that confirms existence of the corporation such as audited annual financial statements or notice of assessment from a municipal, provincial, territorial or federal government.

Additionally, obtain the following information by completing Entity Director/Owner Information sheet:

1. the name and occupation of ALL directors of the corporation; and
2. the name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation (beneficial owners).

To confirm names of corporate directors, the application of incorporation or corporate resolutions mentioning the individuals' names may be referred to.

3.2.2 Entities Other Than Corporations

To confirm the existence of an entity other than a corporation, refer to partnership agreement, articles of association or any other similar record. Obtain the name, address and occupation of all individuals who directly or indirectly own or control 25% or more of the entity (beneficial owners) by completing Entity Director/Owner Information Sheet.

Additional requirements for not-for-profit entities:

1. Determine whether the entity is a registered charity for income tax purposes by asking the account holder and consulting the charities list on Canada Revenue Agency's website http://www.cra-arc.gc.ca;
2. If the entity is not a registered charity, determine whether or not it solicits charitable financial donations from the public, by asking the account holder and documenting it in NAAF.

Ascertain identifications of all individuals authorized to provide instructions on an entity account.

3.3 Third Parties

Complete a Third Party Determination Statement if a third party is involved or if there is reasonable suspicion that a third party is involved. Ascertain the third party's identification when there is certainty of third party's involvement. The third party can be an individual or an entity.

Do not open a non-registered plan (account) if the account holder fails to provide an acceptable identification document. Analyze the information provided by the account holder to determine if there are any logical inconsistencies in the information. Document the identification information provided by the account holder, the method used, unique identifier, expiry date (if any). Do not open a plan (account) for a non-resident individual without a face-to-face meeting between the individual and a financial advisor.

If an account holder either refuses to provide any information required to open up an account or place a transaction when requested, or appears to have intentionally provided misleading information, a financial advisor must immediately notify GPWM supervisory staff. GPWM supervisory staff may make a decision on the issue or refer the issue to the Chief Compliance Officer for further consultations.

3.3 KYC Update

A financial advisor must ask an account holder if they are a PEFP whenever there is a change in the account holder's (i) marital status (ii) occupation.

If an existing account holder is determined to be a PEFP, treat the existing plan (account) as a new plan (account). If the GP NAAF on file is not the most recent version, complete the most recent version and obtain supporting documents/information for re-approval.

4.0 Reviewing Transactions

4.1 Assessing a Suspicious Transaction

An attempted transaction is an incomplete transaction that an account holder intended to conduct and took some form of action, including negotiations or discussions to conduct the transaction and involves concrete measures taken by either GPWM or the account holder.

Evaluate a transaction or an attempted transaction in terms of what seems appropriate and within normal practices of GPWM's business based on Know Your Client (KYC) information when a transaction or an attempted transaction gives rise to discomfort, apprehension or mistrust. Assess the suspicion based on a reasonable evaluation of all circumstances surrounding the transaction, and relevant factors, including the knowledge of the account holder's business, financial history, background, behaviour and indicators mentioned below.

4.1.1 General Indicators

1. Account holder admits or makes statements about involvement in criminal activities.
2. Account holder does not want correspondence sent to home address. Account holder uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
3. Account holder's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact the account holder shortly after opening a plan (account).
4. Account holder appears to have accounts with several financial institutions in one geographical area for no apparent reason.
5. Account holder is accompanied and watched.
6. Account holder shows uncommon curiosity about internal systems, controls and policies.
7. Account holder has only vague knowledge of the amount involved.
8. Account holder is secretive and reluctant to meet in person.
9. Account holder is nervous, not in keeping with the transaction.
10. Account holder is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
11. Account holder is involved in activity out-of-keeping for that individual or business.
12. Inconsistencies appear in the account holder's presentation of the transaction.
13. Account holder appears to have recently established a series of new relationships with different financial entities.
14. Account holder uses aliases and a variety of similar but different addresses.
15. Account holder offers money, gratuities or unusual favours for the provision of services.
16. You are aware that the account holder is the subject of a money laundering or terrorist financing investigation.

4.1.2 Knowledge of Reporting or Record Keeping Requirements Indicators

1. Account holder attempts to convince you not to complete any documentation required for the transaction.
2. Account holder makes inquiries that would indicate a desire to avoid reporting.
3. Account holder seems very conversant with money laundering or terrorist activity financing issues and has unusual knowledge of the law in relation to suspicious transaction reporting.
4. Account holder is quick to volunteer that funds are "clean" or "not being laundered."

4.1.3 Identity Documents Related Indicators

1. Account holder produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
2. Account holder refuses to produce personal identification documents.
3. Account holder only submits copies of personal identification documents.
4. Account holder wants to establish identity using something other than his or her personal identification documents.
5. Account holder's supporting documentation lacks important details such as a phone number.
6. Account holder inordinately delays presenting corporate documents.
7. All identification presented is foreign or cannot be checked for some reason.
8. All identification documents presented appear new or have recent issue dates without any reasonable explanation.

4.1.4 Economic Purpose Indicators

1. Transaction seems to be inconsistent with the account holder's apparent financial standing or usual pattern of activities.
2. Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the account holder.
3. Transaction is unnecessarily complex for its stated purpose.
4. Activity is inconsistent with what would be expected from declared business.
5. Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

4.1.5 Transactions and Account Opening Related Indicators

1. Opening a plan (account) in another individual's name.
2. Opening a plan (account) with a name very close to other established business entities.
3. Attempting to open or operate a plan (account) under a false name.
4. Activity far exceeds activity projected at the time of plan (account) opening.
5. Multiple deposits are made to an account holder's plan (account) by third parties.

4.1.6 Investment Business Specific Indicators

1. Normal attempts to verify the background of a new or prospective account holder is difficult.
2. Account holder attempts to purchase investments with cash.
3. Account holder wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than $10,000, where the transaction is inconsistent with the normal investment practice of the account holder or their financial ability.
4. Account holder uses GPWM as a place to hold funds that are not being used in investment for an extended period of time and such activity is inconsistent with the normal investment practice of the account holder or their financial ability.
5. Account holder frequently makes large investments by cheque within a short time period, which is inconsistent with the normal practice of the account holder.
6. Transfers of funds or securities between plans (accounts) not known to be related to the account holder.
7. Trades conducted by entities that have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
8. Transaction of very large dollar size.
9. Account holder is willing to deposit or invest at rates that are not advantageous or competitive.
10. Account holder exhibits a lack of concern regarding risks, commissions or other transaction costs.
11. Account holder attempts to purchase investments with instruments in the name of a third party.
12. Payments made by way of third party cheques are payable to, or endorsed over to, the account holder.
13. Transactions made by employees of GPWM, or by relatives of such employees, to benefit unknown parties.
14. Transactions in which an account holder makes settlements with cheques drawn by or remittances from a third party(s).
15. Proposed transactions are to be funded by international wire payments, particularly from countries where there is no effective anti-money-laundering system.
16. A new or prospective account holder is known to have a questionable legal reputation or criminal background.

4.1.7 Electronic Funds Transfers Related Indicators

1. An account holder orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
2. An account holder receives large sums of money from an overseas location via electronic funds transfer that includes instructions for payment in cash.
3. An account holder instructs to transfer funds abroad and to expect an equal incoming transfer.
4. An account holder shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.
5. An account holder transfers funds to another country without changing the form of currency.
6. Wire transfers are received from entities having no apparent business connection with an account holder.
7. Size of electronic transfers is out-of-keeping with normal business transactions for that an account holder.
8. Wire transfers do not have information about the beneficial owner or originator when the inclusion of this information would be expected.
9. Stated occupation of the account holder is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).
10. An account holder conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics or that are known for highly secretive banking and corporate law practices.
11. An account holder makes electronic funds transfers to free trade zones that are not in line with the account holder's business.

If an activity seems suspicious, a financial advisor must notify GPWM's Chief Compliance Officer or Compliance Department, providing the account holder's plan (account) particulars, transactions and the nature or reason of suspicion. A financial advisor may continue dealing with the account holder as normal until informed otherwise and would be expected not to inform the account holder of the report or suspicion.

4.2 Transaction Involving Cash or Cash Equivalents

GPWM supervisory staff and financial advisors can not accept cash, traveller's cheques or bearer bonds. GPWM supervisory staff and financial advisors should request a reason behind an account holder not submitting a personal cheque or an entity (account holder) not submitting a corporate cheque or for paying for a purchase with electronically transferred funds, bank draft or money order.

5.0 Record Keeping

Maintain the following records created in the normal course of business or make them readily accessible:

1. account applications including GPWM New Account Application Forms and any supporting attachments or documents including the identification method used, document referred to, unique identifier, and expiry date (if any);
2. transaction Forms;
3. confirmations of purchases and redemptions;
4. Limited Trading Authorizations;
5. Guarantees;

6. Powers of Attorney;
7. Any correspondence, including electronic communications, about the operation of the account holders plan's (accounts);
8. account holder statements sent to the account holder;
9. Third Party Determination Statement, if applicable;
10. Reasons for not paying for a purchase with personal cheque or for making a purchase with electronically transferred funds;
11. Evidence of establishment of source of funds if the account holder has been determined to be a PEFP.

Maintain the following Identification documents (whichever are applicable) or information of an account holder not physically present:

1. Cleared Cheque: Maintain the name of the financial entity and account number of the deposit account on which the cheque was drawn. Preferably keep a legible photocopy of the cheque;
2. Deposit Account Confirmation: Date on which the confirmation was made, name of the financial entity where the account is held and the account number;
3. Identification Product: Name of the identification product, the name of the entity offering it, the search reference number and the date of use of the product to identify the individual;
4. Credit File: Name of the entity keeping the credit file and date of consultation of the credit file;
5. Attestation: Attestation itself;
6. Explanation behind not meeting with the account holder face to face.

Maintain the following for entity accounts:

1. A copy of the record used to establish the existence of the entity and to confirm its name and address. If the record is in paper format, maintain a paper copy of such record on file. If the record is in electronic form, maintain the entity's registration number, the type and source of record and the record must be from a public source.
2. Maintain copies of the part of the official entity records and any amendments thereto showing the provisions that relate to the power to bind the entity regarding the account. Such records include certificate of incumbency, the articles of incorporation, the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller etc., partnership agreement, articles of association or any other similar record;
3. Completed Entity Director/Owner Information Sheet.

Additionally, maintain a copy of the Suspicious Transaction Report when such a report is filed with FINTRAC. Maintain all records for 7 (seven) years from the day of closing of the account to which they relate.

6.0 Risk Assessment and Mitigation

Using the Schedule A of this policy, the Compliance Committee will assess GPWM's risks to money laundering and terrorist financing and determine steps to mitigate such risks. The committee will perform analytic work to review the possibility of money laundering or terrorist financing if such a situation is brought to its attention. There will be additional monitoring of a plan, if the committee deems it necessary.

7.0 Reporting

7.1 Social Insurance Number

Do not provide an account holder's Social Insurance Number to FINTRAC on any type of report.

7.2 Terrorist Property Report

GPWM and its supervisory staff will check the names of an account holder in the GP Wealth Client Management System (Winfund) against the OSFI issued lists available at **http://www.osfi-bsif.gc.ca** before filing the Monthly Report with the Ontario Securities Commission under Section 83.11 of the Criminal Code and under Section 7 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RUINRST) and section 5.1 of the United Nations Al-Qaida and Taliban Regulations (UNAQTR). If a match is found, GPWM and its supervisory staff must investigate the matter further and consult the Compliance Committee if deemed necessary.

If a determination is made that GPWM is in control or possession of property that is owned by or on behalf of anyone on the list, GPWM and its supervisory staff must report its existence to

1. the Ontario Securities Commission (OSC)
2. notify the existence of property as well as any transactions or proposed transactions related to the property to the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS)
3. freeze the account holder's property, that is, prohibit all transactions including redemptions on any plans (accounts).

7.3 Suspicious Transactions Report

Take reasonable measures, before reporting a transaction or an attempted transaction, to identify the individual who conducted or attempted it. Do not identify the individual if

1. already identified and there is no doubt about the identity of the individual; or
2. if doing so would inform the individual that he/she will be reported. Notify GPWM's Chief Compliance Officer or Compliance Department of your suspicion and reason(s) behind such a suspicion.

If an account holder electronically transfers money into an account, parks such funds in a money market fund or other type of investment for a short period of time and then asks the investment to be redeemed/cancelled and money to be paid to him/her or another party, notify GPWM's Chief Compliance Officer or Compliance Department.

GPWM's Chief Compliance Officer or Compliance Department will investigate the matter and file a Suspicious Transaction Report, if deemed necessary, after consultations with the Compliance Committee.

8.0 Testing

The testing of the policy will be conducted every two years either by an outside third party or by an internal officer of GPWM. The following must be reported to the Compliance Committee within 30 days of the testing:

(a) the findings of the testing;
(b) any updates that were made to policies and procedures during the testing period;
(c) the status of implementation of policies and procedures updates.

The report must include a request for a response indicating corrective actions and timelines for implementing such actions.

9.0 Administration

GPWM supervisory staff is responsible for the administration, revision, interpretation and application of this policy. The policy must be reviewed on earlier of

(i) 2 years from the approval date
(ii) changes in law
(iii) significant non-compliance issues
(iv) addition of products/services types offered by GPWM.

10.0 Document Revision History

All revisions made to this document are tracked in the following table.

Date	Author	Revision
June 13, 2008	Mak Sangha	Created
January 12, 2009	Mak Sangha	Revised
August 2, 2011	Paula Sprentz	Combine AML Policy Manual with AML Procedure Manual Change; 1.0 Purpose of Policy to 1.0 Introduction Change; 2.0 Policy to 2.0 Overview of Money Laundering Policy Remove; 5.0 Training moved to 2.10 Training Change; 4.0 Transactions to 4.0 Reviewing Transactions