POLICIES AND PROCEDURES RELATED TO AML / ATF

Last Updated August 2019

TABLE OF CONTENTS

SECTION 1

GENERAL INFORMATION

1.1 Objectives

The present document constitutes the compliance policy adopted by the MAX Financial Ltd., as it concerns the fight against money laundering and the financing of terrorist activities Its objective is to help the managerial staff, employees, financial security advisors and group savings representatives to detect and prevent money laundering and financing of terrorist activities, to respect federal anti-terrorist laws, and to identify and notify of any suspicious activity.

It is important to mention that we are all jointly and severally liable for any breach to the present policy in the eyes of the law.

1.2 Civil and criminal penalties

Offences to the law, to regulations, and to this policy can cause a loss of business and bad publicity for the financial sector, the company and all those for who it is a source of income. These offences may also result in stiff penalties (civil and criminal) and disciplinary measures including dismissal and/or the termination of the contractual relation of all those who have, knowingly or not, violated the laws and regulations on the proceeds of crime (money laundering) and financing of terrorist activities.

SECTION 2

COMPLIANCE

2.1 Compliance program

The law stipulates that a compliance program must be implemented. A program that is well designed and **applied properly by all** can only help us to respect the legal obligations that bind us. Our program includes, amongst others, the following elements:

- The nomination of a compliance agent;
- The creation and application of policies and procedures intended to ensure adhesion to the law;
- A risk evaluation concerning money laundering and financing of terrorist activities, as well as documentation and implementation of risk mitigation measures;
- Creation of an ongoing training program;
- Review of the policies and procedures every two years.

2.2 Adoption of the program

The present policy was approved by MAX Financial Ltd. leadership committee on August 2019 and signed by Mr. Manjinder Singh, its president.

2.3 Recognition of the policy

Recognition of this document by management aims to ensure the credibility of the policy and its accompanying standards for the entire company, in order to ensure that its financial services are not used to promote criminal activities.

MAX Financial Ltd., as well as everyone who is called upon to deal with clients, or become aware of goods belonging to clients or available to them directly or indirectly, will have to comply wholly with the intent of the law and regulations concerning the prevention of money laundering, of financing of terrorist activities and the resulting economic sanctions. We pledge to train the managerial staff, employees, financial security advisors and group savings representatives so that they may comply with these laws and regulations. This obligation also touches all those whose work involves client identification, record keeping and processing of various transactions subject to declaration to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), since under current legislation, we are obligated to:

- Declare suspicious transactions and certain other prescribed transactions as established in section 5 “ SUSPICIOUS TRANSACTIONS ”;

- Implement a compliance program;

2.4 Updates to the program

The standards, procedures, and forms subject to the present can be modified in order to comply with laws, regulations and guiding principles as concerns the fight against money laundering and the financing of terrorist activities. The company’s compliance department, as necessary, will make updates to the present policy, to standards and procedures.

2.5 Persons affected by the program

A copy of the present policy will be distributed to each employee, member of the managerial staff, and to others who are called upon to deal with clients, or become aware of goods belonging to clients or available to them directly or indirectly, so that it may be understood and applied by them. They are obligated to understand its contents and to respect it. They will have to be aware of the context and moments when it is necessary to increase their vigilance levels when executing transactions, for example when dealing with countries or territories who have not yet established programs against money laundering or the financing of terrorist activities that are adequate and respect international standards. Employees, managerial staff, financial security advisors and group savings representatives will have to sign a declaration, which is described in more detail in document A, attached to this policy of through our website.

2.6 Nomination of a compliance agent

Consequently, we have created the position of compliance agent as provided for in regulatory requirements. This person is named in document C, point 1. The length of his/her mandate is indeterminate and the description of his/her tasks is stated in section 3. He/she will also be responsible for updates, support and follow-up of the policy.

The compliance agent will sign a declaration, described in more detail in document B, attached to the present policy.

SECTION 3

COMPLIANCE AGENT

3.1 Responsibilities

The responsibilities of the compliance agent and of senior management are as follows:

- Implement the company's policies and compliance standards as it concerns money laundering and financing of terrorist activities;
- Update this policy;
- Manage this policy and compliance standards by monitoring a strict application of the present policy, for client files as well as for employees;
- Maintain watchfulness mechanisms and submit required revisions to the executive council;
- Establish, supervise and implement training requirements as defined by regulations;
- Establish, supervise and implement a complete risk management policy;
- Study superior level files that are submitted to him/her, solicit additional relevant information and justify his/her evaluation in writing;
- Verify, through relevant techniques, the stringent application of compliance policies and standards;
- Report suspicious transactions or attempts of suspicious transactions according to the standards indicated by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC);
- Maintain in a secure area any relevant element that may be required either by FINTRAC or to demonstrate that all required steps were followed;
- Report his/her activities to the executive council at least once a year. The report will include the following elements concerning his/her activities during the period: surveillance and implementation of these standards and policies, the creation and revision of the policy, its dissemination, the supervision of training requirement as well as the study of and, if necessary, the transmission of contentious files;
- Be excluded from all tasks related to the handling of funds that come through the company;
- Carry out all other incidental tasks related to other professional activities within the company, in connection with his/her employment and as determined by the executive council.

SECTION 4

RISK-BASED APPROACH

4.1 Method used

We will use the “risk-based approach”, which is a process which allows us to identify and measure high risks of money laundering or of financing of terrorist activities, thus allowing us to develop strategies in order to mitigate such risks. Information gathered within the framework of the obligation to verify your clients' identity will be the foundation for this approach. It is the personal responsibility of each financial security advisor, group savings representative and/or other employee affected by this policy to **know his/her client well**.

4.2 Risk assessment

Risk assessment involves analyzing the potential threats and weaknesses that our activities could represent as concerns money laundering and the financing of terrorist activities. We used the following factors in order to document our risk assessment:

- Our products, our services, and the delivery method;
- The geographic location of where we and our clients carry out our activities;
- Other relevant factors that are relative to our company, our clients and the business relations that we have with them.

This assessment was made in two steps:

- **Step 1**: assessment of business risks related to our products, services, delivery methods and geographic locations which may represent a higher risk;

- **Step 2**: assessment of risks related to our business relations with our clients, including products and services that they use and the geographic locations where they carry out their activities.

In Step 1, we created a checklist (appendix D) and a risk table (appendix F). In Step 2, we created a checklist of the most common risk categories (appendix E).

4.2.1 Money laundering

By definition, **money laundering** (or proceeds of crime) means a tentative to conceal or disguise the nature, the location, the source or the control of money obtained by illegal means. When money obtained by illegal means is successfully laundered, criminals retain control over their money and can establish a separate cover for their illegal source of income. Compliance regulations apply to all funds coming from illegal activities (illegal sale of arms, smuggling, drug trafficking, organized crime, prostitution rings, tax fraud, corruption, computer fraud) and held by individuals, associations and groups who try to transfer, spend, and/or invest funds coming from all sorts of criminal activities. Life insurance with a good savings component is an interesting technique for criminals.

4.2.2 The money laundering process

The money laundering process involves three basic steps: placement, layering (dispersion) and integration. Money laundering is not limited to cash money; it also exists as various financial transactions, including money transfers, money orders, cheques, debit cards, credit card transactions and other financial products.

Nominees, “smurfing”, valuable asset purchases with cash, exchange transactions, currency smuggling, gambling in casinos, and black-market peso exchange are some of the methods by which illegally obtained funds can be laundered.

4.2.3 Financing of terrorist activities

The **financing of terrorist activities** provides funds for terrorist activities. A terrorist or a terrorist group is anyone (individual, corporation, trust, etc.) whose object or one of its activities is to engage in or enable terrorist activities. The main objective of terrorist activity is to intimidate a population or compel a

government to do something. Just like a criminal organization, a successful terrorist group must build an effective financial infrastructure. The sums needed for terrorist activities are not always large and the associated transactions are not necessarily complex. The principal methods for collecting funds differ from those used by criminal organizations:

- Support can come from other countries, organizations or rich individuals;
- Money can come from illegal activities;
- Support can be obtained from legitimate sources, such as gifts, etc.

4.3. Risk mitigation

Risk mitigation means the implementation of measures in order to limit potential risk related to money laundering and the financing of terrorist activities described in section 4.2. Although our assessment does not consider that risks are high, we have created a fact sheet which groups three levels in order to help you analyze your client files for money laundering and financing of terrorist activities.

4.3.1 Risk mitigation measures

You must examine three main components as it concerns money laundering and/or the financing of terrorist activities when justified by particular circumstances: the client's reality, the legitimacy of his wealth and the relevance of the transactions. The requirements will be different for each of these three components depending on whether the client is an individual or a company, and a thorough and well-documented administrative process will supervise them. Amongst others, this process will include all relevant questions, as set out in the fact sheet presented in appendix A (individuals) and appendix B (companies), following the three following levels:

- **Green level**

  This covers the vast majority of clients, either because they have been clients for a long time, or because you know them personally, or because they make very few transactions. The requirements are reduced. This is the green level.

- **Yellow level.**

  The file will have to go through a more thorough analysis. It is required for all clients who regularly make a lot of transactions, do business internationally or make a transaction that is exceptional, out of the ordinary or unusual.

- **Red level**

  It is automatically applied to clients who are not Canadian residents, immigrants, and foreign residents as well as all other clients about whom you may have some doubts. **YOU MUST ALWAYS SUBMIT THE FILE TO THE COMPLIANCE AGENT BEFORE MAKING ANY TRANSACTION.**

You will also find appended a reference guide for opening a new client file (appendix C) in order to help you better fight against money laundering and the financing of terrorist activities.

4.3.2 Terrorist status

You must consult the official List of terrorist Entities, available at the following Internet address: http://www.osfi-bsif.gc.ca in order to verify if your client's name appears. It is important to note the date and hour of verification, as well as to print out the document you consulted and keep a copy in your file.

4.3.3 Politically Exposed Foreign Person

Since the 23rd of June 2008, we have to determine if our clients are politically exposed foreign persons. Your client is a politically exposed foreign person if he **holds or has ever held** one of the following offices or positions in or on behalf of a **foreign** country:

- Head of state or government;
- Member of the executive council of government or member of a legislature;
- Deputy minister (or equivalent);
- Ambassador or an ambassador's attaché or counsellor;
- Military general (or higher rank);
- President of a state-owned company or bank;
- Head of a government agency;
- Judge;
- Leader or president of a political party in a legislature.

Also the members of the family of an individual described above that are determined to be:

- The mother or father;
- The child;
- The spouse or common-law partner;
- The spouse's or common-law partner's mother or father;
- The brother, sister, half-brother or half-sister.

In this situation, you will have to take reasonable measures to determine if the client is a “politically exposed foreign person” by asking him the question directly or by consulting a dependable public information source. It is important to specify that as soon as you identify your client as a “politically exposed foreign person”, you must get senior management's approval in order to keep the account open and retain certain documents (see section 7.8.)

4.3.4 Beneficial owner

In order to avoid money laundering and prevent the financing of terrorist activities, you must identify the true account holder and/or owner. For example, the beneficial owner is the person who controls the account, even indirectly.

4.3.5 Cash payment

In order to reduce the risk of money laundering and the financing of terrorist activities, we refuse all payments in cash. Only cheques drawn from the client's bank account and made out in order to the fund and/or insurance company will be accepted in order to purchase financial products and/or insurance. However, it may occasionally happen that a client cheque be made out to “MAX Financial Ltd.

4.4 Monitoring of transactions

The compliance department will establish procedures for the review of unusual, high risk transactions involving transfers in order to identify transactions that could require log keeping or a special reporting procedure, such as filling out the Suspicious Transaction Report, that may later be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) by our compliance department.

4.5 High risk situations for certain sectors

Although our risk assessment (section 4.3) may conclude that the situation is low-risk, there are certain high-risk situations. As a financial entity, securities broker and life insurance representative, the politically exposed foreign person represents a high risk for money laundering and the financing of terrorist activities, as well as any red level situation as set out in appendices A and B of this document. Thus, it is important to determine if the actual holder of the account that represents a high risk is a politically exposed foreign person as described in article 4.3.3. At this time, a review of client files has not revealed any politically exposed foreign persons. A simple way of verifying if your client is a politically exposed foreign person is to ask the question: when opening an account for a new client, or during a meeting for current clients.

If you determine that your client is a politically exposed foreign person and/or you find yourself in a **red** level situation, you must immediately determine the source of the funds and get the approval of management in order to keep the account open.

SECTION 5

SUSPICIOUS TRANSACTIONS

Current legislation obligates financial entities, life insurance representative and securities brokers to declare to FINTRAC any client transaction or recurrent transaction, attempted or completed, that they believe or have reason to believe is:

- An attempt at money laundering; or
- Destined to the financing of terrorism.

5.1 Transactions related to money laundering and the financing of terrorism

A suspicious transaction is a financial transaction that gives rise to reasonable grounds to suspect that it is related to the commission of a **money laundering and/or financing of terrorist activity offence.** This also includes transactions that give rise to reasonable grounds to suspect that it is related to the **attempted** commission of a money laundering and/or financing of terrorist activity offence**.**

“Reasonable grounds to suspect” are established according to what is reasonable from your point of view, including according to current business practices and systems used in our line of business.

It is important to remember that it is the individual's **behaviour** that is suspicious, and not the individual himself, and that it is by taking several factors into account, not just one, that you will be able to determine if there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering or financing of terrorist activity offence or not. All circumstances of the transaction must be examined **on the basis of how well you know the client.**

5.2 How to identify a suspicious transaction

There is no minimum amount for the reporting of a suspicious transaction. Many factors may come into consideration, each one insignificant on its own, but raising doubts when combined. In general, a transaction may be linked to money laundering or the financing of terrorist activity if you find it raises doubts in your mind, makes you uneasy, uncomfortable, worried or mistrustful. Thus we have established three risk levels for the analysis of client files as well as a fact sheet. Please refer to section 4.3 “Risk mitigation ”.

Suspicious activities can vary from one transaction to the next, depending on the circumstances of the client's transaction(s). They can be routine depending on what you know about the client, whereas they may be suspicious for another.

Many factors can be considered when trying to establish if a transaction is particularly suspicious or not, including without being limited to: the amount, the place of transaction, client comments, client behaviour and his transaction history.

Common and sectional indicators can also be useful in judging if a transaction, completed or attempted, is suspicious or not, by examining it with relation to what you know about the client and the risk level category described previously.

5.2.1 Common indicators

The following common indicators **may** help you detect completed or attempted suspicious transactions.

- The client uses an identification document which is false or has visibly been altered;
- The client refuses to present an identification document;
- The client gives you an expired identification document;
- Two or more clients use the same identification document or similar identification documents;
- The client modifies his transaction after you ask for his identification;
- The client voluntarily changes the spelling of his name;
- The client says he does not have a local address, but claims to be a regular client;
- The client deals with two or more advisors and/or mutual fund dealers in order to process simultaneous transactions or make transfers;
- A client makes transactions contrary to his usual activities;
- The client knows the law and the requirements for reporting of suspicious transactions;
- The client mentions that the funds are legal;
- The client gives you suspicious and vague information;

- The transaction involves a fictitious entity, such as a corporation that has no assets and no active sphere of activity.

5.2.2 Industry-specific indicators for life insurance

As an example, here are some indicators related to the life insurance industry in order to help you to assess a situation:

- The client offers to purchase an insurance product and pay with a cheque drawn from an account other than his personal or corporation account;
- The client asks for an insurance product without justification;
- Third parties are involved in the payment of premiums;
- The client cancels an investment soon after purchase;
- The duration of the life insurance contract is less than three years;
- The premium is paid from a foreign account;
- All of the client's principals are located outside of Canada.

5.2.3 Industry-specific indicators for representatives of group savings plan dealers and segregated fund representatives

As an example, here are some indicators related to the group savings and segregated funds industry in order to help you to assess a situation:

- The client attempts to purchase investments with cash;
- Funds or securities are transferred between accounts with no known relation to the client;
- Very large value transactions are made;
- All of the client's principals are located outside of Canada;
- Several clients open accounts within a short period of time to make the same transaction;
- The client is ready to make deposits or investments at rates that are not advantageous or competitive;
- Payments are made by a third party cheque payable to the client;
- Transactions are made in which the client make settlement with cheques drawn by third parties.

5.2.4 Obligation to report

If you have a reasonable grounds to suspect that a completed or attempted transaction is related to the commission, completed or attempted, of a money laundering or financing of terrorist activity offence, **you must not carry out the transaction and report such irregularity to FINTRAC, and this, in all cases. Also consult section 10 " Suspicious Transactions Reports "**.

5.2.5 Failure to report

Failure to report is considered to be a very serious offence and failure to respect our legal obligations can lead to criminal charges with up to five (5) years imprisonment, a fine of up to $2,000,000, or both.

5.3 Terrorist property

Terrorist property means any type of real or personal property that is in our possession or available to us, including any deed or instrument giving title or right to property, or giving right to money, including funds, financial assets, economic resources or merchandise. Here are some examples of what is considered to be assets:

- Cash;
- Bank accounts;
- Insurance policies;
- Money orders;
- Mutual and segregated funds.

The definition of “terrorist group” is stated in section 4.2 Risk assessment. It is important to remember that a terrorist group can be a person, a group, a trust, a partnership, a mutual fund corporation, an organization or an unincorporated association, a non-profit organization or a corporation.

Given the type of activities that we carry out, it is unlikely that we would have terrorist property in our possession or available to us.

However, if during your activities you have reasonable grounds to suspect that a transaction is related to the commission of a money laundering and/or terrorist financing offence, and/or to the attempted commission of a money laundering and/or terrorist financing offence, you must verify with the appropriate authorities if this person's and/or entity's name appears on the Office of the Superintendent of Financial Institutions' list.

In order to dissuade and suppress the financing of terrorist activities, Canada has published lists of names of terrorist entities. Property belonging or available to anyone whose name appears on this list should be blocked and, consequently, any transaction involving such assets is prohibited as well as any transaction related to money laundering and/or the financing of terrorist activities. You may consult this list on the Office of the Superintendent of Financial Institutions' website at http://www.osfi-bsif.gc.ca under “Designated Persons Listings and Sanctions Laws”. You can also consult the Public Safety Canada website at http://www.sp-ps.gc.ca to see if the name and/or group is listed under “Currently listed entities”.

5.3.1 Obligation to report

If you determine that we have in our possession property belonging to a terrorist group, or that it is available to us directly or indirectly, or after a transaction involving such property is completed or planned, **you must not complete the transaction and you must report the irregularities to FINTRAC in all cases and refer to section 11 "Reporting of terrorist group property".**

5.3.2 Failure to report

Failure to report is considered to be a very serious offence and failure to respect our legal obligations can lead to criminal charges with up to five (5) years imprisonment, a fine of up to $2,000,000, or both.

SECTION 6

TRAINING OF PERSONNEL

6.1 Ongoing training

The law, current regulations and/or internal policies of supervisory associations require mandatory and ongoing compliance training for financial security advisors and representatives of groups savings plan dealers. Furthermore, anyone who is in contact with clients, who is aware of transactions made by clients or who manipulates funds is any way, or who is responsible for the implementation or monitoring of the compliance plan must understand the obligation to report, client identification and record keeping. This training is destined to both front line employees and members of senior management. MAX Financial Ltd. is very aware of the importance of these issues, consequently any person involved in client relations and/or in making transactions will have to take a minimum of two hours of training annually.

The main objective of this training is to keep all concerned parties aware of modifications brought to money laundering and financing of terrorist activities legislation, as well as to our policies in order to be aware of the latest developments and upcoming modifications, as part of their work concerning money laundering and the financing of terrorist activities.

The training also applies to any person changing positions within the company and to any new employee, who will immediately receive the necessary training to be familiar with the company's policies and current measures, this to understand the risk of being exposed to money laundering or financing of terrorist activity tactics while carrying out his duties.

Amongst others, the training will allow people to understand record keeping and client identification (section 7), reporting obligations (sections 10 and 11), sanctions in case of non-compliance (section 12) and internal policies and procedures destined to dissuade and detect money laundering and terrorist activity financing practices that may be related to their work.

6.2 Training agent

In order to comply with the present document, as the person named in point 2 of document C will act as training agent; well as training manager and will be responsible for keeping a training log.

The training log will include relevant details (see document D for more information).

SECTION 7

RECORD KEEPING AND VERIFICATION OF CLIENT IDENTIFICATION - GROUP SAVINGS

We pledge to retain all documents required by law and by regulations, particularly but not limited to individuals, for an entity other than a corporation and for accounts used by a third party and/or corporation.

As a representative of a group savings plan broker, you must respect the requirements for record keeping and clients identification described in further detail hereinafter:

- When you open an account;
- During normal account activity;
- When you make a suspicious transaction report;
- When you have to determine the beneficial owners when identifying a corporation.

7.1 Records to be kept for opening an account

7.1.1 Private individual

- The new account application with the signature of the person enabled to give instructions as concerns the account;

7.1.2 Corporation

- The application to open an account, the corporation charter, the resolution stating the officers enabled to sign the new account application and to make transactions;

7.1.3 Other than a corporation

- The new account application, a document containing the name, address, and nature of the principal company or profession practiced.

7.2 Documents created during normal activities

- New account applications;
- Confirmations of purchases or sales;
- Warranties;
- Trade authorizations;
- Current powers of attorney and account agreements;
- Correspondence concerning record keeping, including emails.

7.3 Client account statements

- A copy of all statements sent to clients.

7.4 Documents concerning the reporting of suspicious transactions

- Copy of documents transmitted when sending a report of suspicious transactions to FINTRAC (see sections 10 and 11).

7.5 Documents to ascertain client identity

Although the new account application specifies the type of document used to identify the client, by stating its reference number and where it was issued, client identification is required for opening any new account in the manner described below:

7.5.1 For a private individual

- Birth certificate, driver's licence, passport, landing record, permanent resident card, health card if the client presents it for identification, any document which has a unique identifier number and is issued by a level of government.

7.5.2 For a corporation or a trust

- A certificate of incorporation in paper or electronic form on which the incorporation number, the type and source of the document are

recorded; an annual report signed by an independent audit firm, a letter or notice of assessment issued by a level of government;
- Confirmation of the corporation's directors;
- Ensure that the identification is completed within 30 days of opening the account;
- Shareholder agreement;
- Identification of beneficial owners (persons who can act in the entity's name) in the following manner:
    - Name and profession of all directors;
    - Name, address and profession of any person who holds or controls, directly or indirectly, at least 25% of shares,
    - Information allowing to ascertain the ownership, control and structure of the entity (see Appendix G for reference);
- If we are unable to obtain this information in order to confirm that it is exact as concerns the preceding paragraph, we must:
    - Obtain the name of the chief executive officer of the other entity,
    - Take reasonable measures to confirm the identity of the other entity's chief executive officer,
    - Treat that other entity as high risk in the risk assessment carried out as part of our compliance program.

7.5.3 For an entity other than a corporation

- The shareholder agreement, the articles of association or similar document confirming its existence, in paper or electronic form, and on which the registration number, type and source of the document are recorded;
- Partnership agreement;
- Records of decisions;
- By identifying the beneficial owners (persons who can act in the entity's name) in the following manner:
    - Name, address and profession of any person who holds or controls, directly or indirectly, at least 25% of shares,
    - Information allowing to ascertain the ownership, control and structure of the entity (see Appendix H for reference);
- If we are unable to obtain this information in order to confirm that it is exact as concerns the preceding paragraph, we must:
    - Obtain the name of the chief executive officer of the entity,
    - Take reasonable measures to confirm the identity of the other entity's chief executive officer,
    - Treat that other entity as high risk in the risk assessment carried out as part of our compliance program.

7.5.4 Non-profit organization (NPO)

- In addition to the documents provided for in section 7.5.3, an attestation stating that it is a charitable organization, registered for income tax purposes (consult the list of charitable organization on the Canada Revenue Agency website at http://www.cra-arc.gc.ca) and retain a document to that effect;
- If the organization is not registered, verify if it solicits charitable gifts from the public and retain a document to that effect.

7.6 Business relationship

7.6.1 Definition

A business relationship is the relationship you establish with a client in order to carry out financial transactions or provide services related to these transactions.

A business relationship is established with a client when he makes, within a maximum of five years, two transactions for which you must ascertain his identity.

7.6.2 Information to retain

When we establish a business relationship with a client, we must record, in a document, the planned object of this relationship and the type.

We have to examine this information and keep them current in order to fully understand the client's activities over time and also measure changes in order to detect high risk and, if necessary, take more stringent measures.

The frequency of updates regarding the business relationship information depends on the assessment of the risk your client represents.

7.6.3 Methods of ongoing monitoring for high-risk clients

When we identify a client as high risk, we must increase the frequency of ongoing monitoring and of updates to client identity information, as well as take more stringent measures as necessary.

Here is a non-exhaustive list of more stringent measures we can take in order to mitigate the risks caused by high-risk business relationships as regards our company:

- Obtain additional information about the client;
- Obtain information about the source of the funds or of the client's financial assets;
- Obtain information regarding the reasons for the planned or completed transactions;
- Obtain upper managements' approval to establish or maintain the business relationship;
- Determine trends related to transactions;
- Establish limits for transactions;
- Take additional measures to check documents obtained.

7.7 Third party documents

7.7.1 Definition

Every time that you open a new account, you need to take necessary measures to establish if the account is to be used by a third party or in his name. A third

party is a person or an entity, other than the account holder or the person authorized to give instructions for the account, who manages the account's activities.

If you determine that a third party is involved, you must take reasonable measures to identify such party by researching the information already recorded in the file, with other sources, or directly with the client.

7.7.2 Information to retain

You must keep a document recording the following information:

- Name of the third party, their address and the type of business or profession;
- If the third party is a private individual: the birth date;
- If the third party is a corporation: the incorporation number and the place of issue of the incorporation certificate;
- For the account: the type of relationship between the third party and the account holder.

7.8 Politically Exposed Foreign Person

7.8.1 Definition

Please refer to section 4.3.3 for the definition of a " politically exposed foreign person ". If you have determined that the client is a "politically exposed foreign person", and you have received upper management's approval to keep the account open, you must have a document in which the information described in section 7.7.2 is recorded.

7.8.2 Information to retain

You must keep a document recording the following information:

- What makes the client a "politically exposed foreign person";
- If it is known, the origin of funds deposited or planned to be deposited into the account;
- The date at which you established that the client is a "politically exposed foreign person";
- The name of the member of upper management who authorized the account to remain open;
- The date at which you received authorization to keep the account open.

7.9 Validity of documents and originals

Documents provided must be valid at the time the account is opened and cannot be expired. You must also see the original of each document.

7.10 Update of client identity information

Our risk assessment related to money laundering and the financing of terrorist activities obligates us to take reasonable measures to keep client identity information updated. As part of our activities and in this context, reasonable measures include asking the client to confirm or update this information.

Given our reality, client identification information updates must be made at least every three years. This update also includes directors and shareholders mentioned in sections 7.5.2 and 7.5.3.

7.11 Document retention period

Here is the document retention period according to the type of document:

7.11.1 Account opening and signature cards

They must be retained for seven (7) years following the closing of the account they refer to.

7.11.2 Politically Exposed Foreign Person

They must be retained for seven (7) years following the closing of the account they refer to.

7.11.3 Corporation, other entity and beneficial owners

They must be kept during seven (7) years following the date at which the last commercial transaction was made.

7.11.4 Suspicious transaction reports

They must be retained for seven (7) years after the date the report was submitted.

7.11.5 Other documents

They must be retained for seven (7) years from the date at which they were established.

7.12 SANCTIONS IN CASE OF NON-COMPLIANCE

Failure to keep a document register and to satisfy our legal obligations can give rise to criminal charges: up to five (5) years imprisonment, a fine of up to $500,000 or both. In other words, if you do not respect record keeping or client identification requirements, you expose yourself to administrative penalties.

SECTION 8

RECORD KEEPING AND VERIFICATION OF CLIENT IDENTITY - LIFE INSURANCE

As a financial security advisor, you must respect the requirements for record keeping and client identification described in further detail hereinafter:

- When the client deposits $10,000 or more (whether in cash or not) for the purchase of an annuity or a life insurance policy. You must also keep a client file;
- When the client makes a lump sum payment of $100,000 or more into an immediate or deferred annuity or into a life insurance policy. You must also determine if the client is a politically exposed foreign person (see section 4.3.3);
- When you make a suspicious transaction report;
- When the beneficial owners are determined in the identification of a corporation.

8.1 Documents to keep in the client file

8.1.1 Private individual

- Name, address and the type of principal business or profession;
- Birth date.

8.1.2 Corporation

- A copy of the resolution that includes the names of the representatives enabled to sign for the account.

8.2 Documents concerning suspicious transactions

- When sending a suspicious transaction report to FINTRAC (see sections 10 and 11), you must keep a copy of the documents sent in.

8.3 Documents to ascertain client identity

When you ascertain someone's identity, your file must specify they type of document used for the identification, its reference number and its place of issue. When client identification is required, it must be carried out in the following manner.

8.3.1 For a private individual

- See section 7.5.1

8.3.2 For a corporation

- See section 7.5.2

8.3.3 For an entity other than a corporation

- See section 7.5.3

8.3.4 Non-profit organization (NPO)

- See section 7.5.4

8.4 Business relationship

See section 7.6

8.5 Third party documents

See section 7.7

8.6 Politically Exposed Foreign Person

Applies only if you receive a lump sum payment of $100,000 or more into an annuity or into a life insurance policy. You have 14 days from the transaction date to determine if your client is a politically exposed foreign person.

For information to retain under such circumstances, please refer to sections 4.3.3 and 7.8, which apply to everything that does not comply with the present section.

8.7 Validity of documents and originals

Refer to section 7.9.

8.8 Update of client identity information

Refer to section 7.10.

8.9 Document retention period

Here is the document retention period according to the type of document:

8.9.1 Client files and confirmation of identity

They must be kept during seven (7) years following the date at which the last commercial transaction was made.

8.9.2 Politically Exposed Foreign Person

They must be kept during seven (7) years following the date at which the last commercial transaction was made.

8.9.3 Corporation, other entity and beneficial owners

They must be kept during seven (7) years following the date at which the last commercial transaction was made.

8.9.4 Suspicious transaction reports

They must be retained for seven (7) years after the date the report was submitted.

8.9 Other documents

They must be retained for seven (7) years from the date at which they were established.

8.10 Sanctions in case of non-compliance

Refer to section 7.12.

SECTION 9

AUDIT

9.1 External auditor

The present policy, and the respect of its related standards, will be subject to an audit every two years by an external auditor who is named by the executive committee in a timely manner.

The policies and measures audit will include the following elements:

- Our risk-based assessment of the risk of money laundering and financing of terrorist activities as described in sections 6.1 to 6.5 of FINTRAC's Guideline 4;

- Our training program.

9.2 Control methods

Auditing will be done through controls, interviews and sampling, such as:

- Meetings with persons in charge of carrying out transactions;
- Review of criteria for tracking suspicious transactions and reporting them;
- Verification of the record keeping system in order to confirm its compliance with legal requirements;
- Verification of client identification procedures to confirm their compliance with legal requirements;
- Review of risk assessment.

SECTION 10

SUSPICIOUS TRANSACTION REPORTS

As we are a reporting entity to the intent of the law, this section explains the procedures to follow for filing a suspicious transaction and terrorist financing activity report by paper and which forms are required to do so. Please note that the forms were not reproduced as appendices considering the changes or updates that may be brought to them. However, the forms are available online at http://www.canafe-fintrac.gc.ca (Reporting forms on the Publications page).

10.1 Reporting requirements

We have to report suspicious transactions to FINTRAC once we have reasonable grounds to suspect that a completed or attempted transaction is related to the completed or attempted commission of a money laundering or terrorist activity financing offence (see section 5 on how to recognize this type of transaction) as established in Guideline 3B of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

10.1.1 Reporting timelines

We have **30 calendar days** to present our report with all required and relevant information.

The 30 day period begins as soon as managerial staff, employees, financial security advisors and group savings plan representatives detect a fact about a transaction that constitutes reasonable grounds to suspect that such transaction is related to the commission of a money laundering or terrorist activity financing offence. The 30 period may begin later if the transaction is detected later, that is to say at the time of cognizance of the fact that gives rise to reasonable grounds to believe that an offence has been committed.

10.1.2 Reporting electronically

We have to submit suspicious transactions reports electronically.

10.1.3 Reporter immunity

It is important to note that **all persons involved cannot disclose that they have made a suspicious transaction report, nor disclose its contents with the intent to harm or impair a criminal investigation that may or may not be**

in progress. These persons have immunity, that is to say, they cannot be subject to criminal or civil proceedings for having made a report in good faith.

10.1.4 Designated person for reporting

For the purposes of the foregoing, the company delegates the person named in document C, point 3 as responsible for reporting to FINTRAC.

SECTION 11

REPORTING OF TERRORIST PROPERTY

As we are a reporting entity to the intent of the law, we are obligated to report terrorist property to FINTRAC. You must first verify the lists published in Canada that are available on the Office of the Superintendent of Financial Institutions' website at http://www.osfi-bsif.gc.ca, under the “Designated Persons Listings and Sanctions Laws” section.

11.1 Reporting requirements

There are two situations in which we have the obligation to report terrorist or terrorist group property to FINTRAC. In this section, the notion of “terrorist group” also includes the word “terrorist”.

We are obligated to report:

- When we know that a terrorist group is the **owner** of property or has direct or indirect control over property;
- When we **believe** that the property belongs to a person who is listed on one of the terrorist and sanctions lists or that it is controlled by such a person or in his name, as established in Guideline 5 of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

A listed person (see the following website: http://www.osfi-bsif.gc.ca) means a person, a group, a trust, a partnership, an organization or association which is not a corporation, a non profit organization or a corporation for which there exist reasonable grounds to believe:

- Carried out, attempted to carry out, participated in, or facilitated a terrorist activity;

- Is controlled directly or indirectly by, acts on behalf of, at the direction of, or in association with any individual or entity conducting any of the above activities.

11.1.1 Reporting timelines

If one of the two previously mentioned situations occurs, we must **IMMEDIATELY** submit a terrorist property report, as opposed to a suspicious transaction report.

11.1.2 Reports by paper

The only way to declare is by paper by printing the form available on the following website: http://www.canafe-fintrac.gc.ca, under the "Reporting" section.

11.1.3 Reporter immunity

It is important to note that **all persons involved cannot disclose that they have made a suspicious transaction report, nor disclose its contents with the intent to harm or impair a criminal investigation that may or may not be in progress.** These persons have immunity, that is to say, they cannot be subject to criminal or civil proceedings for having made a report in good faith.

11.1.4 Designated person for reporting

For the purposes of the foregoing, the company delegates the person named in document C, point 3 as responsible for reporting to FINTRAC.

SECTION 12

SANCTIONS
IN CASE OF NON-COMPLIANCE

12.1 Criminal penalties

Failure to satisfy our legal obligations **could** lead to criminal accusations under failure to report a suspicious transaction or terrorist property. A guilty verdict can lead to up to five (5) years imprisonment and/or a $2 million fine or both.

A guilty verdict for failure to meet record keeping requirements can lead to up to five (5) years imprisonment and/or a $500,000 fine or both.

A guilty verdict for failure to establish a compliance program can lead to up to five (5) years imprisonment and/or a $500,000 fine or both.

12.2 Administrative penalties

Failure to implement one of the compliance program's elements as required by law can lead to an administrative penalty of up to $100,000 for each element.

Failure to report required information in the 30 days following the review of the compliance program can lead to an administrative penalty of up to $100,000.

Failure to verify client identity, keep records, monitor financial operations and take measures to mitigate risks in situations where the potential money laundering and terrorist activity financing risk is high can lead to an administrative penalty of up to $100,000.

12.3 Disciplinary penalties

We reserve the right to impose appropriate disciplinary penalties to anyone concerned by the present policy and who breaches it, based on the gravity of the fault. Thus, the penalty could be: a reprimand, suspension without pay, or discharge. The compliance agent will make a recommendation to the executive committee, which will then make the final decision.

SECTION 13
APPENDICES AND DOCUMENTS

Appendix A – Individual

CLIENT'S REALITY	
Level	**Questions**
Green: Official document with photo	Is the client who he claims to be?
Proof of residential address	If yes, do you have proof? If yes, is the client the beneficial owner?
Yellow: passport	Is the client a politically exposed foreign person?
Banking referral	Does the client have a double nationality?
Red: verification by a third party	

LEGITIMACY OF WEALTH	
Level	**Questions**
Green: sources of current income	Is the source of income known?
Source of the balance sheet	Is all income from domestic sources? Does the wealth correspond with the profile?
Yellow: latest notice of assessment	Is the wealth domestic?
Balance sheet certified by the client	Is the client in a high-risk group?
Red: balance sheets with non domestic assets	

TRANSACTION RELEVANCE	
Level	**Questions**
Green: client is the only stakeholder	Is a structure involved?
Usual transactions	Are the deposits normal? Are variations expected?
Yellow: call for a structure	Are the transactions normal?
Large variations in the balance	Are there non-domestic aspects?
Red: transactions with foreign countries and exotic structures	

Appendix B – Company

CLIENT'S REALITY
Level
Green: - Copy of the charter; - Council resolution on the new account application and mention of persons authorized to sign; - Proof of business address in the client's name (P.O. box not valid).
Yellow: - Extract from the government register indicating the company's legal status, its date of creation and the names of shareholders; - A letter of recommendation issued by a Canadian financial institution bearing the client's name, his civic address, and the length of the relationship with the client.
Red: - Mostly for companies whose address is not in Canada.

LEGITIMACY OF WEALTH
Level
Green: • Interview process; • Wealth profile form (mandatory).
Yellow: • An audited statement of financial position for the last full year, with a provisional balance sheet if the statement of financial position was issued more than six months ago; **AND** • The company's audited statement of income and expenses for the last full year, with a provisional statement if the statement was issued more than six months ago.
Red: – Mostly for companies whose address is not in Canada.

TRANSACTION RELEVANCE
Level
Green: – Must fill out the transaction profile.
Yellow: – Must provide, for each transaction, a written explanation or justification for the transaction.
Red: – Mostly for companies whose address is not in Canada.

Appendix C – Opening a client file

This appendix is a reference tool for opening a client file. Any other additional verification method you may use in respect of the law can only be beneficial to our money laundering and financing of terrorist activity policy.

1. Check for terrorist status;

2. Check for politically exposed foreign person status;

3. Check for beneficial owner status;

4. Validate documents bearing photos;

    a. Always see the original;
    b. Check the validity period and expiration date;
    c. Certify the provided documentation as follows:

    "I hereby certify that I saw the original of this document. I am able to identify the client I met from the photo. In witness whereof, I have signed.

    Name:_____ Signature:_____Date:_____"

5. Validate the other documents

    a. Validate the date of issue of the document if issued less than 90 days ago;
    b. Keep the original on file.

6. Banking referral

    a. Verify that the letter respects the following requirements:
        - Issued within the last 90 days;
        - Name of client;
        - Name of financial institution;
        - Client reliability;
        - Client address;
        - Original signature;
        - Client since X number of years;

Document A – Employee declaration

DECLARATION OF THE EMPLOYEE, MANAGERIAL STAFF, FINANCIAL SECURITY ADVISOR AND REPRESENTATIVE OF A GROUP SAVINGS PLAN BROKER

I, _____ working as a _____, born on the ____ of the month of _____ of the year_____in_____, acknowledge that I have taken cognizance and received a copy of the compliance policy and of the standards that stem from it.

I solemnly pledge to respect my duty of compliance, to report, without delay, any suspicious transaction, to avoid wilful blindness, and to respect current laws, regulations and standards, including this policy and its future modifications

In witness whereof, I have signed on _____

_____
SIGNATURE

_____
WITNESS

Document B – Compliance agent declaration

I, _____ working as a _____, born on the ____ of the month of _____ 19___, in_____, acknowledge having been given the mandate, by management, to act as compliance agent and this for as long as such mandate is not revoked.

I solemnly pledge to abide by my compliance duties as described in section 3 of MAX Financial Ltd. compliance program, amongst others, to implement and manage our compliance policy, to manage training and to report suspicious transactions to regulatory authorities with the required independence.

In witness whereof, I have signed on _____

_____
SIGNATURE

_____
WITNESS

Document C- Responsible persons

Point 1: Compliance agent and responsible for updates, support and follow-up

_____

Point 2: Training agent and responsible for the training record

_____

Point 3: Responsible for reporting to FINTRAC

_____

Document D– Sample of the training record

Training date: _____

Participant name: _____

Training title: _____

Accreditation (CSF and/or IQPF): _____

Providing firm: _____

Creator/trainer: _____

Training description: _____

_____

_____

Number of hours: _____

Subject: _____

APPENDIX D – Products, services, service delivery channel, and geographic location

The following checklists are intended to provide a way to assess risk as concerns our products, services, service delivery channels and our geographic locations. This list corresponds to our company's personality and this risk assessment tool was created on the basis of our particular business requirements.

If we answer “yes” to one of the questions below, we have to consider this element as presenting a higher risk of money laundering or of terrorist financing activities. If necessary, we must take appropriate mitigation measures.

Do we offer one of the following products, services, or service delivery channels:	YES	NO	N/A
For all sectors			
Do we offer services that make it difficult to ascertain the client's identity?			
Do we offer electronic payment services?			
Do we offer the following services: • Electronic money? • Fund transfers (national or international)? • Automated teller machines (ATM)?			
For financial entities Do we offer the following services: • International correspondent bank services for transactions such as commercial payments for persons who are not clients (for example as an intermediary bank) and services of carriers or couriers for international transport of cash, monetary instruments or other documents? • Services involving banknote and precious metal trading and delivery? • Electronic banking services? • Private banking? • Foreign correspondent accounts? • Financing of foreign trade (letters of credit)? • Lending activities, particularly loans secured by cash collateral and marketable securities? • Non-deposit account services? • Accounts through which you can extend bank			

draft writing privileges to the clients of other institutions, often foreign banks? • Services involving an immigrant investor program? • Non face-to-face transactions, such as Internet services, by mail or by telephone?			

Do we deal with clients and offer products or services in the following geographic locations?	**YES**	**NO**	**N/A**
For all sectors			
Is the client located in a known high crime rate area?			
Do we or our clients operate in the following geographical locations: • Any country subject to sanctions, embargoes or similar measures issued by, for example, the United Nations, or in certain circumstances, to sanctions or measures similar to those issued by the UN, but which may not be universally recognized. • Any country identified as a financial secrecy haven or jurisdiction? • Any country identified by the Financial Action Task Force (FATF) as a high-risk jurisdiction in the fight against money laundering or terrorist financing or subject to a FATF statement? • Any country identified by credible sources as: ○ Lacking appropriate money laundering or terrorist financing laws and regulations? ➢ Providing financing or support of terrorist activities? ➢ Having significant levels of corruption or other criminal activities?			

APPENDIX E – Clients within and clients outside of business relationships

The following checklist is intended to provide a way to assess risk for your clients, both within business relationships and outside of them. This list corresponds to our company's personality and this risk assessment tool was created on the basis of our particular business requirements.

If we answer “yes” to one of the questions below, we have to consider this element as presenting a higher risk of money laundering or of terrorist financing activities. If necessary, we must take appropriate mitigation measures.

	YES	NO	N/A
For all sectors			
Does our client operate a cash intensive business?			
Does the client’s business generate large amounts of cash for certain transactions that are not normally cash intensive?			
Is the client an intermediary or "gatekeeper" such as a professional that holds accounts for clients where the identity of the underlying client is not disclosed to you?			
Does the client use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering or anti terrorist financing obligations?			
Does client identification take place other than face-to-face?			
Does the client reside outside Canada?			
Does the client deal offshore?			
Is the client an unregistered charity or other unregulated “not for profit” organization (that can operate on a cross-border basis)?			
Is the client located in a known high crime rate area?			
Has the client been identified as engaging in activity that is consistent with indicators for suspicious transactions?			
Does your client's knowledge of local laws, regulations and rules seem excessive?			
Is this a new client?			
Does the client use intermediaries (corporations, trusts, foundations, partnerships) or other structures seem unusual, complex or unnecessary for their			

business?			
Does the client's structure or nature of its business make it difficult to ascertain the identity of the true owners or controllers?			
Are you unable to obtain beneficial ownership information for your client (if your client is a corporation, trust or other entity)?			
Is there a significant and unexplained geographic distance between the client and us?			
Is there frequent and unexplained movement of funds or accounts towards different geographic locations or institutions?			
Is the client a politically exposed foreign person? See section 4.3.3			

APPENDIX F – FINTRAC risk assessment level table

We have used the following matrix, as appropriate, to assess money laundering or financing of terrorist activity risks associated to our products, services and clients. This table is inspired by one included in a document about risk-based approach published by the Financial Action Task Force (FATF).

Low	Moderate	High
Your client base is stable and well known.	Your client base is increasing due to new branches or to mergers or acquisitions.	Your client base, which is already large, is increasing in diverse geographic areas.
You do not offer electronic transaction services or the website is informational and non-transactional.	You are beginning electronic transaction services but only offer limited products and services.	You offer a wide array of electronic transaction services (such as account transfers, or accounts opened via the Internet).
You do few or no important currency transactions.	You make a moderate number of large currency or structured transactions.	You make a significant number of large currency or structured transactions.
You have assigned a high-risk level to very few clients or businesses you do business with.	You have assigned a high-risk level to a moderate number of clients or businesses you do business with.	You have assigned a high-risk level to a large number of clients or businesses you do business with.
You only have a few international accounts or very low volume of currency activity in these accounts.	You have a moderate number of international accounts for which currency activities are unexplained.	You have a large number of international accounts for which currency activities are unexplained.
You make very few fund transfers or transactions for third parties. You don't make any foreign fund transfers.	You make a moderate number of fund transfers, with a very limited number of international transfers for business or personal accounts, involving low-risk countries.	You make a significant number of fund transfers, with a very limited number of international transfers for business or personal accounts, to and from high risk countries known as financial secrecy havens.
Your business is located in	Your business is located	Your business is

an area known to have a low crime rate.	in an area known to have a moderate crime rate.	located in an area known to have a high crime rate.
You do not make transactions with high-risk geographical locations.	You make very few transactions with high-risk geographical locations.	You make a significant number of transactions with high-risk geographical locations.
The turnover of key personnel in your anti-money laundering program, or of front line personnel (representatives, cashiers, and other similar personnel) in charge of service delivery, is low.	The turnover of key personnel in your anti-money laundering program is low, but your front line personnel in charge of service delivery may have changed.	The turnover of personnel is high, especially for key positions in your anti-money laundering program.

Taken from FINTRAC Guideline 4, appendix 3

APPENDIX G- Ownership, control and structure of a corporation and/or trust

Here is an example of ownership, control and structure of a corporation:

“ABC Québec Inc. is a for-profit corporation, incorporated pursuant to the *Business Corporations Act of Québec* with 100 privately traded shares in circulation. John Ford owns 15 shares and the XYZ Company Inc. owns 85 shares. John Doe is the president of the board of directors, his wife Julie is the secretary, their son Julian is the chief financial officer and his two children are the other members of the board of directors.”

In the example, for a corporation:

- Ownership of the corporation is shared by John Ford (15% of shares) and the XYZ Company Inc. (85% of shares);

- The members of the Board control the company, as does the XYZ Company Inc. which owns 85% of shares;

  In a case like this, you must research further into the ownership until you find an individual who owns enough shares of the XYZ Company Inc. to own or control 25% or more, or until you find that there no such individual;

- The structure of the corporation is that of a privately traded, for-profit corporation incorporated pursuant to the *Business Corporations Act of Québec*;

- The articles of incorporation should provide this information. If you are unable to obtain the names and addresses of all directors or persons who control or own, directly or indirectly, at least 25% of the corporation's shares, you must find the name of the corporation's chief executive officer, that is to say, the person who is responsible for managing this corporation.

If the entity is a trust:

- The names and addresses of all trustees and all known beneficiaries and settlors of the trust;

- The information on the ownership, control and structure of the trust.

- The deed of trust should provide this information. If you are unable to obtain the names and addresses of the trustees, beneficiaries or settlors of the trust, you must find the name of the senior managing officer of the trust, that is, the person in the trust company who is in fact responsible for the management of that trust.

APPENDIX H- Ownership, control and structure of an entity OTHER than a corporation or trust

Here is an example of ownership, control and structure of an entity other than a corporation or trust:

“Argent Comptant Pro is a money services business (MSB) in Sherbrooke. The owners, Albert and Ginette, paid a lawyer to draft a partnership agreement for the business, which they both signed. According to the agreement, Albert will invest the upfront capital in the amount of $50,000 to purchase the franchise and equipment. Ginette will be responsible for operating the partnership and its activities. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. If they decide to end the partnership, Albert will be refunded his upfront capital and the rest of the proceeds from the sale of assets will be split 50% - 50% with Ginette.”

In this example:

- Ownership of the entity is shared between Albert and Ginette;
- Albert and Ginette both control the partnership;
- The structure of the entity is a partnership constituted pursuant to a contract governed by the laws of Quebec.