SNOWCAP FINANCIAL LIMITED

ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING POLICY

1 June, 2025

Introduction.

SnowCap Financial Limited ("SnowCap") is committed to detecting and deterring persons engaged in money laundering or terrorist financing activities by complying with anti-money laundering ("AML") and anti-terrorist financing ("ATF") and economic sanctions laws and regulations ("Applicable Law") and all other best practices associated with its registration as a money services business ("Money Services Business" or "MSB") under the supervision of and reporting to the Financial Transactions and Reports Analysis Centre ("FINTRAC") of Canada.

Our AML and ATF compliance program ("Compliance Program"), as established under this policy and the relevant resolution of the company's board of directors ("Board of Directors"), is designed to ensure compliance with all applicable regulations and MSB rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business. In Canada, the primary regulation is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 ("PCMLTFA"). FINTRAC is Canada's financial intelligence unit that assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. SnowCap recognizes that money laundering can occur in three stages. First, cash enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders, or deposited into accounts at financial institutions. Second, at the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. Third, at the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Compliance Program.

As set out herein, the Compliance Program includes:

- the appointment of a Chief AML Officer ("CAMLO");
- oversight of the program by senior management and the Board of Directors;
- policies and procedures that address regulatory requirements;

- a risk assessment;
- client identification;
- ongoing monitoring;
- regulatory reporting;
- a training program and training plan;
- record keeping; and
- testing the effectiveness of the program every 2 years.

Governance.

[Name of person] is the CAMLO for SnowCap.

The CAMLO is responsible to senior management and the Board of Directors of SnowCap for establishing and maintaining SnowCap's AML Program. This AML and ATF Policy is subject to review and approval by the [Board of Directors].

Risk Assessments.

A firm risk assessment will be conducted and developed based on its business activities. The firm risk assessment will consider the following factors:

- products, services and delivery channels;
- geographic locations of business and clients;
- clients and business relationships;
- use of technology; and
- domestic and foreign affiliates.

Controls and measures have been adopted to mitigate risks and handle identified risks. These controls include keeping client identification information up to date and conducting enhanced monitoring for high-risk clients.

A client risk assessment is completed for each relationship to determine the risk level of the client and whether enhanced monitoring is required. Risk may be based on the client's geographic location, products used and other factors specific to the client such as occupation.

Client Identification.

A business relationship is established with a client at the time an account is opened. Through the MSB Know-Your Client and suitability rules, SnowCap establishes the intended nature of the relationship, the intended use of the account, and keeps client information up to date. In addition to the information collected under MSB Know-Your Client and suitability rules, SnowCap must also meet the client identification requirements under the PCMLTFA.

You must verify the identity of every person for whom you open an account and every person who is authorized to give instructions on an account before the first transaction is carried out on the account, other than the initial deposit. You must also verify the identity of every corporation and entity other than a corporation for which you open an account, within 30 days after the day on which the account is opened.

You cannot open an account for a person, corporation, or other entity if you cannot verify their identity.

(a) Identifying Persons.

You may verify the identity of a person by referring to a government-issued photo identification document. To do so, the document must:

- be authentic, valid and current;
- be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document);
- indicate the person's name;
- include a photo of the person;
- include a unique identifying number; and
- match the name and appearance of the person being identified.

You can determine whether a government-issued photo identification document is authentic, valid and current by viewing it in person, and by looking at the characteristics of the original physical document and its security features (or markers, as applicable) in the presence of the person being identified. This will allow you to be satisfied that it is authentic, as issued by the competent authority (federal, provincial, or territorial government), valid (unaltered, not counterfeit) and current (not expired).

If you are unable to meet with the client in person, you may verify their identity by using the dual-process method, which consists of doing any two of the following:

- referring to information from a reliable source that includes the person's name and address and confirming that the name and address are those of the person;
- referring to information from a reliable source that includes the person's name and date of birth, and confirming that the name and date of birth are those of the person; or
- referring to information that includes the person's name and confirms that they have a deposit account, or a credit card or other loan account with a financial entity and confirming that information.

The information you refer to must be valid and current and come from two different reliable sources. This information could be found in statements, letters, certificates, forms or other information sources that can be provided through an original version or by another version of the information's original format such as a fax, a photocopy, a scan, or an electronic image. For example, you can rely on a fax, photocopy, scan or electronic image of a government-issued photo identification document as one of the two pieces of information required to verify a person's identity.

You cannot use the same source for the two categories of information you choose to verify a person's identity.

If you use the government-issued photo identification method, you must record:

- the person's name;
- the date on which you verified the person's identity;
- the type of document used (*e.g.*, driver's licence, passport, *etc.*);
- the unique identifying number of the document used;
- the jurisdiction (province or state) and country of issue of the document; and
- the expiry date of the document, if available (if this information appears on the document or card, you must record it).

- If you use the dual-process method to verify a person's identity, you must record:
- the person's name;
- the date you verified the information;
- the name of the two different reliable sources that were used to verify the identity of the person;
- the type of information referred to (for example, a utility statement, a bank statement, a marriage licence); and
- the number associated with the information (*e.g.*, account number or if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, *etc.*). If you use information aggregated by a Canadian credit bureau and receive information from two distinct sources (tradelines), you must record the account number or number associated to each tradeline, not the aggregator (credit bureau) number.

(b) Identifying Entities.

To verify the identity of a corporation, you may refer to:

- a certificate of incorporation;
- a record that has to be filed annually under provincial securities legislation; or
- the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors, such as a certificate of active corporate status, the corporation's published annual report signed by an audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial, or federal government.

You may obtain a corporation's name and address and the names of its directors from a publicly accessible database, such as a provincial or federal database like the Corporations Canada database, or a corporation search and registration service through subscription.

When a corporation is a public company, you do not need to confirm the names of its directors when you confirm its existence.

To verify the identity of an entity other than a corporation, you may refer to:

- a partnership agreement;
- articles of association; or
- the most recent version of any other record that confirms its existence and contains its name and address.

The record you refer to must be authentic, valid, and current. If you refer to a paper record or an electronic version of a record, you must keep the record or a copy of it. If the electronic version of the record that you refer to is contained in a database that is accessible to the public, you must keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.

(c) Beneficial Ownership.

SnowCap must make reasonable efforts to obtain, verify the accuracy of, and record information regarding the beneficial ownership of entities. For corporations and other entities, the names and addresses of all individuals who, directly or indirectly, own or control 25% or more of the shares of the corporation or entity should be recorded. In addition, the organizational structure of the entity should be recorded. If it is not possible to obtain beneficial ownership information, SnowCap should

identify the most senior managing officer of the entity, record the reasonable measures taken to obtain beneficial ownership information, and treat the entity as high-risk and subject to enhanced monitoring.

(d) Third Party Determination.

SnowCap must take reasonable measures to determine whether an account is to be used by or on behalf of a third party. When opening an account, a third party is an individual or entity other than the account holder or those authorized to give instructions about the account, who directs what happens with the account.

The following information must be obtained and recorded with respect to the third party:

- if the third party is a person, the third party's name, address, telephone number, date of birth, and occupation, or in the case of a sole proprietor, the nature of the principal business;
- if the third party is a corporation or other entity, the third party's name, address, telephone number, the nature of the principal business, its registration or incorporation number and the jurisdiction and country of issue of that number; and
- nature of the relationship between the client and the third party.
- If you are unable to obtain and record the information above, you must note the following:
- the reason(s) why it is suspected that a third party was involved;
- whether the client indicated on the account opening documents that the account would only be used by or on behalf of an account holder; and
- whether the client indicated the transaction was (or was not) on behalf of a third party.

(e) Politically Exposed Persons and Heads of International Organizations.

SnowCap must take reasonable measures when identifying each client to determine if the individual, or an immediate family member or close associate, is a foreign or domestic politically exposed persons ("PEP") or a heads of international organizations ("HIO"). For definitions of foreign PEP, domestic PEP, HIO, immediate family member and close associate, refer to Appendix 1.

Determining whether a client is a PEP or HIO is done by inquiring at the time of account opening and by screening individual names using a commercial database at account opening and on a periodic basis for existing account holders. The determination should be made within 30 days of opening an account and within 30 days of identifying a fact about an existing account holder that provides reasonable grounds to suspect that the account holder is a foreign PEP, domestic PEP or HIO.

Foreign PEPs must be designated as high-risk clients and within 30 days of the determination you must obtain approval from the CAMLO to maintain the account. Domestic PEPs and HIOs will be assessed to determine whether to be treated as high-risk. Considerations include geographic location of the PEP/HIO, source of funds, or any other relevant information.

Records must be kept of the following information related to PEPs and HIOs:

- the office or position of the PEP or HIO;
- name of the organization or institution of the PEP or HIO;
- the source of funds for the account;
- the source of wealth (*i.e.*, accumulated net worth)

- the date it was determined the individual was a PEP or HIO;
- relationship with the client if the PEP or HIO is an immediate family member or close associate; and
- approval for maintaining the account.

Monitoring.

During the period of a business relationship with a client, ongoing monitoring must be conducted to detect any suspicious transactions, to assess the level of risk associated with a client's transactions and activities, to determine whether transactions or activities are consistent for the client and to keep client information up to date.

The frequency of monitoring depends on the risk level assigned to the client. You should refer to SnowCap's Risk Assessment document for a more detailed analysis and procedures for monitoring based on risk. Individuals who are Domestic or Foreign PEPs will be subject to more frequent monitoring.

Reporting.

(a) Suspicious Transaction Reporting.

A suspicious transaction report ("STR") must be submitted to FINTRAC as soon as practicable after completing the measures required to establish reasonable grounds to suspect that a transaction is related to the commission or the attempted commission of a money laundering/terrorist activity financing offence. The report must be filed whether the transaction was carried out or simply attempted.

It is the consideration of many factors, not any one factor, that may lead to a conclusion that there are reasonable grounds to suspect that a transaction is related to a money laundering or terrorist financing offence. Advisors and Compliance staff are often in the best position to identify indicators or red flags that could initiate suspicion. You must consider the client's usual behaviour and account activity and be alert to transactions or activity which is inconsistent with the client's normal [investment] practices. Indicators may relate to any of the following:

- identifying the person or entity (*e.g.*, difficulty in obtaining information or inconsistencies in documents);
- client behaviour (*e.g.*, Client is nervous or defensive, provides confusing details about a transaction);
- surrounding transactions (*e.g.*, volume of transactions is inconsistent with the client's apparent financial standing, client appears to be living beyond their means);
- types of products and services — multiple accounts internally or externally with no apparent reason, accounts used for pass-through activities;
- changes in account activity or atypical transactional activity (*e.g.*, a change in ownership of a business with no explanation, an inactive account becomes active, abrupt change in activity, a series of complicated transfers); or
- requests for wire transfers or transactions involving non-Canadian jurisdictions (*ex.*, client is unaware of incoming wire transfers, client sends or receives frequent wire transfers, client moves funds immediately after transfer clears, transactions involving countries deemed high-risk or non-cooperative by Financial Action Task Force).

Any suspicious transactions must be immediately reported to the CAMLO. Once the required information is obtained, Compliance will file the STR electronically to FINTRAC. Filing an STR is confidential. It is not permitted to notify the client or any other party that may be involved in the transaction.

(b) Large Cash Transaction Reporting.

Large cash transactions must be reported to FINTRAC when a cash amount of $10,000 or more is received in a single transaction or a series of transactions within a 24-hour period for the same client.

SnowCap does not accept cash transactions. Any cash presented by a client should be returned to the client, and payment by cheque or other acceptable method should be requested.

(c) Terrorist Property Reporting.

Any property in SnowCap's possession or control that is known or believed to be owned or controlled by or on behalf of a terrorist or terrorist group is subject to freezing the account, notifying the Royal Canadian Mounted Police ("RCMP") and the Canadian Security Intelligence Service and the immediate filing of a Terrorist Property Report with FINTRAC.

The Compliance department, in coordination with the CAMLO, is responsible for terrorist property reporting.

(d) Sanctions Reporting.

Similar to terrorist property filing above, SnowCap is required to freeze the account and report to the RCMP any property for sanctioned individuals or entities under the *Special Economic Measures Act*, S.C. 1992, c. 17 ("SEMA") or other applicable U.N. sanctions. Note that there is no requirement to report to FINTRAC.

The Compliance department, in coordination with the CAMLO, is responsible for sanctions reporting.

(e) Monthly Reporting to Principal Regulator.

SnowCap must prepare and submit the Monthly Suppression of Terrorism and Canadian sanctions Report by the 14th of each month to its principal regulator. The monthly report should only include the true positive matches under the *Criminal Code*, R.S.C. 1985, c. C-46 ("Criminal Code") and the *Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)*, S.C. 2017, c. 21 ("JVFCOA"). It should not include any true positive matches under the SEMA, other U.N. sanctions, or the *Freezing Assets of Corrupt Foreign Officials Act*, S.C. 2011, c. 10. Where there a no true positive matches, a "nil" report is still required under the Criminal Code and the JVFCOA. Nil reporting is not required in respect of other regulations under the *United Nations Act*, R.S.C. 1985, c. U-2.

Record Keeping.

The PCMLTFA and associated Regulations require an SnowCap to meet record keeping requirements. Generally, you must keep records for five years from the day they were created.

Records which must be retained include:

- account opening and client identification records;

- PEP and HIO documentation;
- records related to ongoing monitoring including the information obtained from the monitoring;
- suspicious transaction reports;
- terrorist property reports;
- large cash transaction records and reports; and
- records related to AML training.

Directives.

SnowCap monitors for Ministerial Directives by subscribing to electronic updates from FINTRAC and ensures that any Directives are identified and actioned as required.

Training.

SnowCap provides training to all new hires as part of the onboarding process.

In addition, as part of the annual Compliance training delivered to the firm, employees receive training on SnowCap's AML obligations including the establishment of the Compliance Program, client identification, transaction monitoring and reporting, PEP determinations and anti-terrorist and sanctions screening.

Records evidencing completion of training are maintained by the Compliance department.

Review of Compliance Program.

SnowCap's Compliance Program is subject to review by internal audit at least once every 2 years. Internal audit will review for effectiveness of the program including whether policies, procedures and the risk assessment are comprehensive and up to date, whether adequate records are maintained as required under the regulations, and that an effective training program and plan is in place with training being conducted on a regular basis. In addition, SnowCap's Compliance Program may be subject to review by FINTRAC.

Appendix 1 Politically Exposed Persons

Foreign PEPs.

A foreign PEP is an individual who holds or has held one of the following offices or positions in or on behalf of a foreign country, regardless of citizenship, resident status or place of birth:

• head of state or head of government;

• member of the executive council of government or member of a legislature;

• deputy minister or equivalent rank;

• ambassador, or attaché or counsellor of an ambassador;

• military officer with a rank of general or above;

• president of a state-owned company or a state-owned bank;

• head of a government agency;

• judge of a supreme court, constitutional court or other court of last resort; or

• leader or president of a political party represented in a legislature.

Where a person is determined to be a foreign PEP, they will always remain a foreign PEP, including after they are deceased.

Domestic PEPs.

A domestic PEP is defined an individual who holds or has held (within the last 5 years) one of the following offices or positions in or on behalf of the Canadian federal, provincial or municipal government as follows:

• Governor General, lieutenant governor or head of government;

• member of the Senate or House of Commons or member of a legislature;

• deputy minister or equivalent rank;

• ambassador, or attaché or counsellor of an ambassador;

• military officer with a rank of general or above;

• president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;

• head of a government agency;

• judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;

• leader or president of a political party represented in a legislature; or

• mayor of a city, town, village, rural or metropolitan municipality.

A person ceases to be a domestic PEP 5 years after they have left office or 5 years after they are deceased.

Heads of International Organizations.

An international organization is defined as an organization established by the governments of more than one country, or an institution established by an international organization. The head of such an organization is considered the primary person who leads that organization, such as president or chief executive officer.

A person ceases to be an HIO 5 years after they are no longer the head of the organization or institution or 5 years after they are deceased.

Family Members and Close Associates.

Immediate family members and close associates of a foreign or domestic PEP or HIO are also considered to be PEPs and HIOs respectively. The following are considered immediate family members of a PEP or HIO (including biological and adopted family members):

• spouse or common-law partner;

• ex-spouse or common-law partner;

• child;

• parent;

• the parent of the spouse or common-law partner; and

• child of their parent (sibling or half-sibling).

The following are considered close associates of a PEP or HIO:

• business partners, or individuals who beneficially own or control a business with a PEP or HIO;

• a person in a personal or romantic relationship with a PEP or HIO;

• a person involved in financial transactions with a PEP or a HIO;

• a prominent member of the same political party or union as a PEP or HIO;

• a person serving as a member of the same board as a PEP or HIO; or

• a person closely carrying out charitable works with a PEP or HIO.